Information
and Privacy
Commissioner/
Ontario

National Security in a Post-9/11 World:

The Rise of Surveillance ... the Demise of Privacy?

Green College
University of British Columbia

Ann Cavoukian, Ph.D.
Commissioner

May 2003

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca

This publication is also available on the IPC Web site.

Table of Contents

Introduction 1

Initiatives 2

United States 2

USA PATRIOT Act 2

Operation "TIPS" 3

Homeland Security 4

Terrorism Information Awareness 5

Computer Assisted Passenger Prescreening System 6

Domestic Security and Enhancement Act 7

Canada 8

Anti-terrorism Act, Bill C-36 8

Advance Passenger Information/Passenger Name Record 9

Public Safety Act, Bill C-17 11

Lawful Access 12

Identity Cards 13

Concerns 15

General Concerns 15

Expanded Scope of Domestic Surveillance 15

Lack of Justification 16

Rush Job 17

Lack of Openness 18

Weakening or Elimination Judicial Controls 19

Lack of Oversight 21

Economic Risks 22

Not Effective 22

Vulnerable and Complicated Technology 23

Tempting Target 24

Too Much Information 25

Wasted Resources 26

Easy to Exploit 26

Solving the Wrong Problem 28

Civil Liberties Concerns 29
Unconstitutional 29
Freedom of Speech and Political Association 31
Presumption of Innocence 32
Search and Seizure 32
Due Process 33
Equal Protection 34
Fair and Public Trial 35

Privacy Concerns 35
Big Brother 37
Loss of Autonomy 38
Loss of Anonymity 39
Lack of Consent and Knowledge 40
Necessity and Relevance of Personal Information 40
Unrelated Use and Disclosure 42
Data Quality 44

Privacy versus National Security 45

New model 47

Minimize Impact on Privacy 48
Justification 49
Effectiveness 52
Limiting Purposes 52
Accountability 54

Conclusion 56

Notes 58

Introduction

The devastation of the September 11, 2001, terrorist attacks had a profound impact on people around the world. The Canadian and United States governments immediately made public safety and national security their highest priority, quickly passing sweeping anti-terrorism legislation that dramatically expanded police and surveillance powers. New controls on physical movement and identity verification were imposed at border crossings and airports. In addition, the possibility of introducing compulsory identity cards and biometrics returned to the public policy debate.

In that time of crisis, national security became the paramount consideration, even if privacy and civil liberties had to be sacrificed. However, now the public has started to cool to the idea of national security at all costs. At the beginning of 2002, a Quebec television show asked: "In the name of security, would you accept intrusions in your private life?" Of the 400 viewers who called or e-mailed, 85% answered "no."[1]

In the post-9/11 world, it is difficult to discuss privacy and national security in the same breath. These are very serious, difficult, and emotional issues. When privacy is raised during a national security debate (both personal and political), inevitably some one poses a question like: "Would you rather keep your personal information private than be safe from a car bomb?"

The problem with such a question, and much of the rhetoric surrounding anti-terrorism initiatives, is that it sets up an unreasonable equation – privacy or national security – either/or. The reality however, is not either/or. Even if countries move to completely extinguish privacy, they will still not be completely safe from terrorist attacks.

Given this frightening knowledge, democratic governments must determine the value of privacy to their societies and how it can be protected as they grapple with the difficult issues surrounding national security.

The Office of the Information and Privacy Commissioner/Ontario (the IPC) has a mandate under the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* to offer comment on government legislation and programs, to research matters affecting access and privacy, and to conduct public education. In pursuit of that mandate, the IPC reviewed the national security measures introduced since the 9/11 attacks, concerned with the impact they have had, and will continue to have, if left unchecked.

Accordingly, the purpose of this paper is to provide an introduction to the main anti-terrorist initiatives, to create a greater awareness of the concerns (technical, civil liberty and privacy) being raised about these measures, and to outline the factors we believe governments should consider to ensure that surveillance technologies and other national security systems are implemented in a manner that minimizes the impact on privacy.

Initiatives

Following the terrorist attacks of September 11, 2001, democratic governments around the world responded swiftly by introducing legislation designed to enhance their national security and their ability to fight terrorism. On October 24, 2001, the United States passed the *USA PATRIOT Act*. On October 31, 2001, France passed 13 anti-terrorism measures. On November 13, 2001, the United Kingdom introduced the *Anti-Terrorism, Crime and Security Act*, which became law on December 15, 2001. Canada passed the *Anti-Terrorism Act*, which became law on December 18, 2001. Australia introduced a package of five anti-terrorism bills called the *Security Legislation Amendment (Terrorism) Act, 2002*.

The discussion below focuses on the legislative response of the federal governments of the United States and Canada. It also highlights several other significant anti-terrorism initiatives being contemplated.

United States

USA PATRIOT Act

On October 26, 2001, the United States Congress passed the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (*USA PATRIOT Act*). The next day, President Bush signed it into law. The *USA PATRIOT Act* broadly expanded the powers of United States federal law enforcement agencies to investigate cases involving foreign intelligence and international terrorism.

The most significant and powerful provisions of the law allow for:

- **Expanded Surveillance:** The *USA PATRIOT Act* greatly expanded the scope of traditional tools of surveillance, such as wiretaps and pen registers/trap and trace. Surveillance measures under the *Foreign Intelligence Surveillance Act* (FISA) relating to spying in the United States by foreign intelligence agencies were also expanded.

  The *USA PATRIOT Act* significantly increased the type and amount of information the government can obtain about users from their Internet Service Providers (ISPs). It permits ISPs to voluntarily give law enforcement all "non-content" information without requiring a court order or subpoena. It also expanded the records the government may seek with a simple subpoena (no court review required) to include records of session times and durations, temporarily assigned network (IP) addresses, means and source of payments, including credit card or bank account numbers.[2]

- **Easy access to records:** Under the legislation, the Federal Bureau of Investigation (FBI) can require anyone to turn over records on their customers or clients. This gives the United States' federal government unparalleled power to access and review individuals' financial records, medical histories, Internet usage, travel patterns, and other records.

- **Expansion of the exceptions in wiretap law:** The law expanded exceptions to the normal requirement for probable cause in wiretap law. Now the FBI need not show probable cause or even reasonable suspicion of criminal activity prior to a wiretap.

- **Secret searches:** Under what is known as "sneak and peek" search warrants, the government can conduct searches without notifying the subjects until long after the search has been executed.

- **Increased information-sharing between domestic law enforcement and intelligence agencies:** Restrictions on American foreign intelligence agencies from spying on United States citizens and on the exchange of information were reduced. The *USA PATRIOT Act* allows for wiretap results, grand jury information and other information collected in criminal cases to be disclosed to intelligence agencies when the information constitutes foreign intelligence.[3]

Several provisions of the *USA PATRIOT Act* will expire on December 31, 2005 unless renewed by Congress. The sunset provision does not apply to the sharing of grand jury information with the Central Intelligence Agency (CIA), secret searches, or extended application of the pen register and trap-and-trace law to the Internet. Nor does it apply to ongoing investigations.[4]

Operation "TIPS"

In 2002 the Bush Administration proposed an initiative called the Terrorism Information and Prevention System. Known as Operation TIPS, it was to be part of a new volunteer Citizen Corp program. A pilot project was scheduled to start in August 2002, with one million informants participating in the first stage.[5]

The Citizen Corp Web site described the program as follows:

> Operation TIPS will be a national system for reporting suspicious, and potentially terrorist-related activity. The program will involve the millions of American workers who, in the daily course of their work, are in a unique position to see potentially unusual or suspicious activity in public places. ...
>
> All it will take to volunteer is a telephone or access to the Internet as tips can be reported on the toll-free hotline or online. Information received will be entered into the national database and referred electronically to a point of contact in each state as appropriate. ...

> The goal of the program is to establish a reliable and comprehensive national system for reporting suspicious, and potentially terrorist-related, activity. By establishing one central reporting center, information from several different industries can be maintained in a single database.[6]

TIPS volunteers were to be recruited primarily from among those whose work provided access to homes, businesses or transport systems. Letter carriers, utility employees, truck drivers and train conductors were among those named as targeted recruits.[7]

The TIPS program drew such fierce criticism that its proposed scope was scaled back. The Justice Department announced the program would not involve workers who could enter private property, such as utility workers and mail carriers, but still would involve truckers, dock workers, bus drivers, and other who are in positions to monitor public places. In November 2002, however, Congress said no – it included a provision in the *Homeland Security Act* prohibiting the further development of Operation TIPS.

Homeland Security

The *Homeland Security Act* (HSA) was signed by President Bush on November 25, 2002. It created a new Cabinet-level Department of Homeland Security (DHS) that consolidated 22 agencies into one department with 170,000 employees.

The areas transferred to DHS include the Coast Guard, Customs Service, Secret Service, new Bureaus of Border Security and Citizenship and Immigration, and the Federal Emergency Management Agency. The HSA left the FBI and the CIA untouched, except for the transfer of the FBI's National Infrastructure Protection Center and other computer security entities to the DHS.

One of the Department's main roles is to access, receive and analyze information collected from sources including intelligence agencies, law enforcement, and the private sector in order to identify and assess terrorist threats. It will also produce "watch lists" which contain names of persons suspected of some involvement in terrorism, though not wanted for arrest.[8]

The HSA included the *Cyber Security Enhancement Act*, which has a provision that expands the ability of ISPs to voluntarily disclose information to government officials. The content of e-mail messages or instant messages can be given to a government official in an emergency, without requiring a factual basis stated for the emergency or imminent threat of injury.[9]

Terrorism Information Awareness

On November 20, 2002, the Pentagon announced its intention to have the Information Awareness Office (IAO) of the Defense Advanced Research Projects Agency (DARPA), undertake research initiatives designed to detect terrorists.[10] The program, which had been called Total Information Awareness, has since been renamed to Terrorism Information Awareness (TIA). It was not created or authorized by the HSA.

According to the DARPA Web site, the goal of the TIA program is:

> ... to revolutionize the ability of the United States to detect, classify and identify foreign terrorists – and decipher their plans – and thereby enable the U.S. to take timely action to successfully preempt and defeat terrorist acts.[11]

According to an undated report entitled *Defense Advanced Research Projects Agency's Information Awareness Office and Total Information Awareness Project*, the IAO is developing an experimental prototype system that consists of three parts: 1) language translation technologies, 2) data search and pattern recognition technologies, and 3) advanced collaborative and decision support tools.[12]

A key component of the TIA project is to develop data mining tools capable of sorting through massive amounts of information to find patterns and associations. John Poindexter, Director of IAO, said the TIA will "break down the stovepipes" that separate commercial and government databases. It would give the American federal government the power to generate a comprehensive data profile on any United States citizen.[13]

According to Robert Popp, IAO's Deputy Director, in order to plan and execute their attacks, terrorists must conduct everyday transactions – buy supplies, purchase airline tickets, and make phone calls. Those transactions leave a record that can be detected and the TIA system will look at transaction records for patterns that might point to a terrorist scenario.[14]

> As a broad example, consider the perpetrators of the Sept. 11 attacks. Some of their names were on government lists of suspected terrorists. Many of them had bank accounts and residences in the United States. If federal officials could have been alerted that some of the men were placing calls to one another, enrolling in the same flight schools and purchasing airline tickets for the same day, a proverbial red flag might have given them away.
>
> Before those dots of information can be connected, they have to be found, and that's the first step of the TIA system. It would use a variety of technological components – such as information search-and-retrieval tools or programs that automatically translate recorded messages – to sift out related dots from the daunting volume of information held mostly in private sector databases.[15]

DARPA acknowledged concerns about accessing information normally off limits to the government. Reportedly, it is experimenting with ways to anonymize data.[16] According to John Poindexter, the TIA system would "ensure that the private information on innocent citizens is protected."[17]

Another component of TIA will be the development of biometric technology to enable the identification and tracking of individuals. DARPA already funds the "Human ID at a Distance" program, which aims to positively identify people from a distance using face or gait recognition.[18]

At the end of January 2003, the United States Senate undertook a voice vote to stop all funding for the TIA program until the Pentagon can prove to Congress that the program does not violate the privacy rights of Americans. At the time of writing, the measure had passed the Senate by a 100-0 vote and won concurrence in the House.[19]

The measure would require the Pentagon to report to Congress on the goals of the program, including recommendations from the Attorney General on minimizing the impact on civil liberties. The measure also would keep the Pentagon from deploying the program or transferring it to another department, such as the FBI or the HSD, without congressional authorization. These limitations would not apply if the deployment or transfer of technology was being made for lawful foreign intelligence activities or military operations outside the United States.[20]

Computer Assisted Passenger Prescreening System

Over 639 million passengers pass through airports annually in the United States.[21] As part of its efforts to increase air travel security, the United States Transportation Security Administration (TSA) plans to develop a profiling system that uses a network of "supercomputers" intended to instantly assess every passenger's background to identify potential ties to terrorism.

CAPPS II, which is short for the second-generation Computer Assisted Passenger Prescreening System, will analyze passengers' travel reservations, housing information, family ties, credit reports and other personal information in order to determine if they are a potential threat.[22]

The new system builds upon an existing profiling system known as the Computer Assisted Passenger Screening (CAPS) system. Operational industry-wide in the United States since 1998, CAPS was in use on September 11, 2001.[23]

CAPS involved the collection of data on passengers prior to their boarding a plane. The information was entered into a computer database that determined whether the passenger posed a potential security risk and, as a result, should be subjected to heightened security procedures. Different profiles were to be employed depending upon whether the travel was domestic or international.[24]

Post-9/11, CAPS was seen as suffering from several critical weaknesses including the fact that while it could inform authorities of a passenger's travel pattern, there was no mechanism for a more detailed evaluation. Industry security analysts saw the need for a next-generation version of CAPS that included a central data warehouse.[25]

According to TSA and industry sources, the system will be designed to conduct "real-time preflight background threat evaluation" of airline passengers by using names and personal information taken from passenger manifests. It will compare information from manifests with information collected and analyzed from "numerous databases from government, industry and the private sector" to determine whether any passengers pose a security threat.[26]

CAPPS II will be accessible at all points of passenger processing: booking, ticketing, check in, security screening and aircraft boarding. It also will serve as a repository for information such as biometric data for registered passengers and airport employees.[27]

Transportation and intelligence officials intend to extend the use of CAPPS II to screen truckers, railroad conductors, subway workers and others whose transportation jobs involve the public trust.[28]

A September 2002 report in the *Washington Post* indicated the project had been slowed down by the complexity of the task.[29] However, at the beginning of March 2003, it was reported that Delta Air Lines was to begin testing "a new government plan for air security" that will "check background information and assign a threat level to everyone who buys a ticket for a commercial flight." Delta will try the system out at three undisclosed airports.[30]

Domestic Security and Enhancement Act

In February 2003, the Center for Public Integrity posted a draft of the *Domestic Security and Enhancement Act*, which has been dubbed the PATRIOT Act II. This Bill was prepared by the Bush Administration despite Justice Department officials denying they were drafting another anti-terrorism package to members of the Senate Judiciary Committee.[31] At the time of writing, the Bill had not been introduced into Congress. The Bill's provisions include:

- Non-citizens could be deported even if they had not committed any immigration violations.
- The *Freedom of Information Act* would be amended so that the public would be restricted from obtaining the identification of detainees.
- The United States Attorney General could authorize wiretaps on individuals for 15 days with no court order pursuant to certain actions by Congress or the President.
- DNA samples could be collected from anyone suspected of being a terrorist even if that person had not committed a crime.[32]

Canada

Anti-terrorism Act, Bill C-36

Introduced on October 15, 2001, and passed by the House of Commons in November 28, 2001, *An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism* (*Anti-terrorism Act*) received Royal Assent on December 18, 2001.

The *Anti-terrorism Act* amended the federal *Access to Information Act*, *Privacy Act*, and *Personal Information Protection and Electronic Documents Act* to remove information from the operation of these statutes if the Attorney General of Canada issues a secrecy order prohibiting the disclosure of information because it may harm international relations, national defence or security.

Bill C-36 amended the *Criminal Code* to include a definition of "terrorist activity." It includes an interpretive clause clarifying that an expression of political, religious or ideological beliefs alone is not a "terrorist activity," unless it is part of a larger conduct that meets all of the requirements of the definition (i.e., conduct that is committed for a political, religious or ideological purpose, is intended to intimidate the public or compel a government, and intentionally causes death or serious physical harm to people).[33]

The *Anti-Terrorism Act* includes several provisions that authorize secret court hearings, prohibit disclosure of the identity of participants in proceedings, and conceal the contents of evidence from the accused. These are departures from the previous general rule that court hearings are open to the public and the press, the identity of all witnesses, lawyers and judge are public, and the accused is permitted to see and hear all evidence against him or her.

More significantly, in terms of surveillance, the legislation gives law enforcement and national security agencies new investigative tools to gather knowledge about and prosecute terrorists and terrorist groups.

Significant changes to the *Criminal Code* include:

- **Grounds for obtaining authorization to wiretap:** Amendments eliminated the need to demonstrate that electronic surveillance was a last resort in the investigation of terrorists.
- **Duration of wiretap order:** Amendments enable a wiretap order to be extended for up to one year when used to investigate suspected terrorist activities, instead of a time limit of 60 days, as for most offences.
- **Delay of notification of person whose communications have been intercepted:** The *Anti-Terrorism Act* added "terrorism offences" to the list of circumstances in which an Attorney General may delay notifying persons subject to wiretap of an interception for up to three years.

New provisions permit the Minister of National Defence to authorize the Communications Security Establishment (CSE) to monitor and intercept electronic communications within Canada for the purpose of gathering intelligence.

Initially, Bill C-36 did not contain a sunset clause, but after considerable opposition it was amended so that provisions dealing with preventive arrest and investigative hearing powers will sunset after five years unless a resolution is passed by both the House of Commons and Senate to extend these powers for up to five more years.[34] In addition, the whole Act is subject to a Parliamentary review three years after passage.

Advance Passenger Information/Passenger Name Record

According to a Fact Sheet put out by Citizenship and Immigration Canada (CIC):

> After September 11, the Government of Canada recognized the benefits of receiving passenger information before an international flight arrives in Canada. The Canada Customs and Revenue Agency (CCRA) and CIC have been working in close partnership to put the Advance Passenger Information (API) system in place.
>
> By receiving information before the flight arrives, Canadian Passenger Analysis Units (CPAUs) – made up of Canadian customs and immigration officers – will be able to verify whether anyone on the flight is of concern. Passengers who are of concern will be referred for an in-depth interview.
>
> We will also undertake a similar initiative with our U.S. counterparts.[35]

Since December 31, 2001, all air carriers flying into the United States are required to provide API on all passengers and crew. Mexico started a voluntary program and may launch a mandatory initiative in the coming year.[36]

CCRA's Advance Passenger Information/Passenger Name Record (API/PNR) initiative was announced in April 2000 as part of the Customs Action Plan. The enabling regulations took effect October 7, 2002, and apply to all passengers flying into Canada on commercial airlines.[37]

The air passenger database will be extended to cruise ships, ferries, trains and buses. A CCRA spokesperson confirmed that passengers on ships and trains will be included in the database starting in 2003, while advance screening of bus and ferry passengers will be more difficult. Since it is not necessary to give a name when purchasing a ticket, bus and ferry screening will not start until 2004 or beyond.

At the last point before passengers depart for Canada, the API/PNR system requires travel agents, commercial air carriers and charterers, and any owner or operator of a reservation system, to provide CCRA officials with specific information on all passengers and crewmembers en route to Canada.

The following "customs information" must be provided:

- surname, first name and any middle names;
- date of birth;
- gender;
- citizenship or nationality;
- type of travel document used for identification;
- name of the country that issued the travel document;
- number of the travel document;
- reservation record locator number, if any, and, in the case of a person in charge of the commercial conveyance or any other crew member without a reservation record locator number, notification of their status as a crew member; and
- information relating to the person in a reservation system.[38]

Reports indicate travel destinations, form of payment, seat selection, number of pieces of baggage and ticket booking date will also be maintained in CCRA's database.[39]

CCRA customs enforcement data is currently kept for six years. This standard has been agreed to by the United States under the Smart Border Action Plan. The use of API/PNR data is covered under section 107 of the *Customs Act*, which authorizes the release of customs information to other agencies and departments for specified public policy purposes.

The Privacy Commissioner of Canada and seven of his provincial and territorial counterparts objected to many of the above provisions. On April 8, 2003, Revenue Minister Elinor Caplan wrote the federal Privacy Commissioner and detailed a number of changes that had been made to the API/PNR system, including:

- PNR information to be held for six years, but use and access will be different during 4 (overlapping) time periods:
  - First 72 hours: no change in uses and disclosures previously announced;
  - From 72 hours to 2 years, information will be shared with regulatory agencies for customs purposes and law enforcement agencies in pursuit of border offences, without a warrant, but shared with other law enforcement agencies only with a warrant (including tax officials in CCRA);

- From 72 hours to 2 years: information depersonalized and used without names also by intelligence officials for risk assessment and on-going customs investigations. Name can be reattached to information when necessary for customs purposes;

- From 3 to 6 years, information can only be used for security of Canada, not all customs purposes. The information is used on a depersonalized basis unless the CCRA Commissioner personally approves re-personalizing it based on reason to suspect need to do this to deal with a high-risk person;

    - During this period, information shared only with agencies having a national security or defence mandate and only where grounds for belief in a real or apprehended threat.[40]

Public Safety Act, Bill C-17

Bill C-17, the *Public Safety Act, 2002*, received first reading in the House of Commons on October 31, 2002, and second reading on November 20, 2002. At the time of writing, the Bill had not proceeded further.

The Bill replaces Bill C-55, which died on the Order Paper in September 2002. Bill C-55, in turn, replaced Bill C-42, which was given first reading in November 2001, but was withdrawn by the Government after it received significant criticism.

According to a Government of Canada news release, the proposed *Public Safety Act, 2002* will increase the federal government's capacity to prevent terrorist attacks, protect Canadians, and respond swiftly should a significant threat arise.[41]

Amendments under Bill C-55 would have given responsible ministers the authority to issue an interim order if immediate action was required to deal with a serious threat or significant risk – direct or indirect – to health, safety, security, or the environment. Orders would have been issued in circumstances where there was no regulation or inadequate regulation to address such a threat.[42]

Much of the criticism about Bills C-42 and C-55 focussed on this provision because it was thought to give ministers too much power without sufficient Parliamentary oversight. These provisions are retained in Bill C-17, but the responsible minister must obtain approval from Cabinet within 14 days, and a copy of the order has to be tabled in the House of Commons and Senate within 15 days, regardless of whether Parliament is in session.

One of the most controversial provisions of Bill C-55 related to requirements about passenger information. Amendments to the *Aeronautics Act* would have provided authority for the Royal Canadian Mounted Police (RCMP) and Canadian Security Intelligence Service (CSIS) to obtain information from air carriers and ticket agencies, and to data match it in ways that went beyond securing against terrorism (e.g., to follow arrest warrants).

Bill C-17 removes the provision in Bill C-55 allowing designated RCMP officers access to passenger information for the primary purpose of identifying individuals with a warrant for their arrest. RCMP officers may access passenger information only for the purpose of transportation security, and CSIS officers may do so only for the purposes of national and transportation security.[43]

However, if the RCMP "incidentally" discovers that a passenger had an outstanding warrant for a serious crime, the RCMP is authorized to tell other law enforcement agencies that the passenger is on the plane. According to the federal government, retaining this aspect of the scheme is "necessary for reasons of public safety because the RCMP needs to take appropriate action if it happens to find a passenger wanted for an outstanding warrant for a serious offence such as murder or kidnapping."[44]

Lawful Access

On August 25, 2002, the Government of Canada released a consultation paper setting out proposals to improve what it called "lawful access" by amending several Canadian statutes, including the *Criminal Code* and the *Competition Act*, in preparation for ratifying the Council of Europe's *Convention on Cybercrime*.

The proposals are intended to "update the existing legal framework to help law enforcement and national security agencies address the challenges posed by advanced communications and information technologies."[45]

The federal government argues that:

> For law enforcement and national security agencies, lawful access is an essential tool in the prevention, investigation and prosecution of serious offences and the investigation of threats to the security of Canada. Lawfully authorized interception and the search and seizure of documentation, computer data, and other information is used frequently by law enforcement agencies to investigate serious crimes such as drug trafficking, child pornography, murder, money laundering, price fixing and deceptive telemarketing. National security agencies utilize lawfully authorized interception to investigate terrorist and other threats to national security.[46]

Two key proposals in the Government of Canada's consultation document are:

- **Infrastructure capability:** It was proposed that all service providers (wireless, wireline and Internet) be required to ensure their systems have the technical capability to provide lawful access to law enforcement and national security agencies.

- **National database of customer information:** One of the problems identified in the consultation papers was the deregulation of the telecommunications market had created delays for law enforcement in identifying the local service provider and getting subscriber information.

> To address this problem the establishment of a national database and a requirement for service providers to submit accurate and current customer information to it was proposed. Australia, the Netherlands and Germany have established databases or statutory means for law enforcement and national security agencies to obtain accurate subscriber and service provider information quickly. In these countries, telecommunications service providers are required to provide such information and are responsible for its accuracy, completeness and currency.[47]

The federal government received over 300 submissions in response to the consultation paper. According to one source, the Departments involved recognized that more consultation was necessary prior to proceeding with legislative amendments.[48]

Identity Cards

In the Fall of 2002, Denis Coderre, Canada's Citizenship and Immigration Minister suggested "a high-tech national identity card" should be studied by the federal government. This issue has come up a number of times in recent years. For example, in 2000, the federal government dismissed consideration of a national identity card to replace the Social Insurance Number because of public concerns about privacy and a potential cost near $3.6 billion.[49]

Minister Coderre's vision of an identity card would include a biometric, such as fingerprints or optical scan, which he believes would make it more difficult for a terrorist to steal someone's identity or fabricate a fraudulent version of the card. Minister Coderre made this proposal at a time when the United States changed its policy to require Canadian citizens born in Middle Eastern countries to be fingerprinted and photographed, and was considering requiring Canadian landed immigrants from Commonwealth countries to carry visas when crossing the border.[50]

Citizenship and Immigration Canada already has the Permanent Resident Card designed "to increase border security, improve the integrity of the immigration process, and provide holders with secure proof of their permanent residence status when re-entering Canada on any commercial carriers (plane, train, boat, and bus)." As of December 31, 2003, individuals with permanent residence status will need to show their Permanent Resident Card when returning from international travel on commercial carriers.[51]

The House of Commons Standing Committee on Citizenship and Immigration undertook to study the national identity issue and invited comments on the following issues:

- What are the existing problems with Canadian identity documents, particularly "foundation" documents such as birth certificates?
- What should be the guiding principles for a national strategy on identity documents?
- Which level(s) of government should be responsible?

- Do we need to create a new national identity card, or can the security features of existing "foundation" documents be strengthened?
- What has been the experience of other countries with national identity cards?
- Should everyone in Canada be required to carry a secure identity document at all times? Or should the identity document be voluntary for some (e.g., Canadian citizens and permanent residents) and mandatory for others (e.g., refugee claimants, foreign students, or other temporary residents)?
- What information should be imbedded in the cards, who should be able to access that information, should the information be stored centrally, and what safeguards would be required to prevent misuse?
- What technologies are available for enhancing document security and what issues are raised by the use of particular technologies, such as biometrics? (Biometric identifiers include fingerprints, iris scans and facial scans).
- How much would a national identity card cost? What savings would be realized by introducing such a card (e.g., reduction in crime related to identity theft)?[52]

At the time of writing, the outcome of the consultation remains unknown.

Concerns

Criticism about anti-terrorism legislation and other measures in the United States and Canada focussed on three main areas: 1) general concerns about the scope and effectiveness of these initiatives, 2) violations of civil liberties, and 3) invasions of privacy.

General Concerns

Expanded Scope of Domestic Surveillance

One of the main criticisms of the post-9/11 anti-terrorism initiatives is their overly broad scope, resulting in widespread surveillance of the general public. In Canada, this issue was the focus of much criticism for the proposed *Public Safety Act, 2002*. In his comments about Bill C-17, the Privacy Commissioner of Canada stated:

> This is unprecedented. The Government of Canada has absolutely no business creating a massive database of personal information about all law-abiding Canadians that is collected without our consent from third parties, not to provide us with any service but simply to have it available to use against us if it ever becomes expedient to do so. Compiling dossiers on the private activities of all law-abiding citizens is the sort of thing the Stasi secret police used to do in the former East Germany. It has no place in a free and democratic society.[53]

In the United States, the Center for Democracy and Technology (CDT) was particularly concerned about the *USA PATRIOT Act* because many of its provisions were not limited to terrorism investigations but rather applied to all criminal or intelligence investigations. Specifically, the CDT noted that the Act:

- allows government agents to collect undefined new information about Web browsing and e-mail without meaningful judicial review;
- allows ISPs, universities, network administrators to authorize surveillance of "computer trespassers" without a judicial order;
- allows law enforcement agencies to search homes and offices without notifying the owner for days or weeks after, not only in terrorism cases, but in all cases;
- allows FBI to share with the CIA information collected in the name of a grand jury, thereby giving the CIA "the domestic subpoena powers it was never supposed to have;" and
- allows FBI to conduct wiretaps and secret searches in criminal cases using the lower standards previously used only for the purpose of collecting foreign intelligence.[54]

The Electronic Frontier Foundation (EFF) also expressed the view that the "Attorney General seized upon the legitimate Congressional concern following the September 11, 2001, attacks to pad the USAPA [*USA PATRIOT Act*] with provisions that have at most, a tangential relationship to preventing terrorism."[55] The EFF argued that a number of the amendments were targeted at "low and mid-level computer defacement and damage cases" which, although clearly criminal, are "by no means terrorist offenses."[56]

The proposed TIPS program in the United States drew immediate criticism because of the unprecedented scope of the domestic surveillance that it would have authorized – the program would use a minimum of 4% of Americans to report suspicious activity.[57]

Perhaps the most aggressive expansion of domestic surveillance is being proposed under the TIA initiative. A major concern is that it would combine every American's bank records, tax filings, driver's license information, records at credit card purchases, medical data, and phone and e-mail records into one giant, centralized database. This would then be combed through for evidence of any kind of suspicious activity.

Critics fear the chilling effect such widespread surveillance will have on society. It is thought the existence of TIA will impact the behaviour of both terrorists and law-abiding individuals alike. Terrorists are likely to go to great lengths to make certain that their behaviour is statistically "normal," while ordinary people are likely to avoid unusual but lawful behaviour out of fear of being labelled "un-American."[58] As one critic noted: "The program wouldn't catch terrorists, but it would terrorize ordinary citizens by logging their every movement in a federal government database."[59]

Lack of Justification

Concerns about the dramatic increase in the scope of surveillance in Canada and the United States were compounded by a lack of justification for such actions. Governments failed to demonstrate why these new measures were necessary to fight terrorism and enhance national security and most importantly, whether they would be effective. Critics of the anti-terrorism legislation argued the need and benefits presented by government were overstated and unsubstantiated.

At the time the *USA PATRIOT Act* was introduced the EFF stated:

> ... in asking for ... broad new powers, the government made no showing that the previous powers of law enforcement and intelligence agencies to spy on US citizens were insufficient to allow them to investigate and prosecute acts of terrorism. The process leading to the passage of the bill did little to ease these concerns. To the contrary, they are amplified by the inclusion of so many provisions that, instead of aimed at terrorism, are aimed at non-violent, domestic computer crime. In addition, although many of the provisions facially appear aimed at terrorism, the Government made no showing that the reasons they failed to detect the planning of the recent attacks or any other terrorist attacks were the civil liberties compromised with the passage of [the *USA PATRIOT Act*].[60]

Canada's Privacy Commissioners and consumer groups were quick to question the justification for the wide-ranging powers proposed under the lawful access consultation paper. The federal Privacy Commissioner noted:

> ... what is being requested here are significantly new and enhanced powers of access to the private communications of Canadians that go far beyond maintaining the capabilities and authorities that law enforcement and national security agencies may have had in the past.
>
> What's missing is evidence demonstrating that there is, in fact, a serious problem that needs to be addressed. Lacking any evidence of serious problems requiring correction by invading the privacy of Canadians, it is not possible to be persuaded that the proposals address these problems effectively, proportionally, and in the least privacy-invasive manner possible.[61]

Rush Job

In both Canada and the United States one of the first waves of protest over anti-terrorism legislation was the speed with which they were passed. The *USA PATRIOT Act* was passed just six weeks after the September 11 attacks, with Canada's *Anti-terrorism Act* being passed 14 weeks after the attacks.

Many critics felt the broad scope and complexity of these statutes, combined with no formal consultation and extremely short time frames for public reaction precluded informed debate and comprehensive analysis of their provisions.

When introduced, the *USA PATRIOT Act* was 342 pages long and made changes to over 15 different statutes. As the EFF noted:

> ... it is a large and complex law that had over four different names and several versions in the five weeks between the introduction of its first predecessor and its final passage into law. ... it seems clear that the vast majority of the sections included have not been carefully studied by Congress, nor was sufficient time taken to debate it or to hear testimony from experts outside of law enforcement in the fields where it makes major changes. This concern is amplified because several of the key procedural processes applicable to any other proposed laws, including inter-agency review, the normal committee and hearing processes and thorough voting, were suspended for this bill.[62]

The Canadian Centre for Policy Alternatives (CCPA) levelled the same criticism against Bill C-36, noting there was no opportunity to ask and have answered key questions such as:

- Is the Bill necessary in order to combat terrorism?
- Has the government demonstrated satisfactorily that existing domestic legislation, including the *Criminal Code*, the *Immigration Act*, the *National Defence Act*, the *Security Offences Act* and the *Official Secrets Act*, is not adequate?

- Will the measures in Bill C-36 make Canadians safer?
- Are there not more effective responses, such as better enforcement of existing laws and measures to improve communication between, for example, the RCMP and the Canadian Security Intelligence Service?
- Will key provisions of the Bill withstand scrutiny under the *Canadian Charter of Rights and Freedoms*?
- Will Canadians have to challenge any rights' violations at a high personal and financial cost?[63]

Lack of Openness

Critics remain concerned because details about both the scope and operation of a number of initiatives are limited or unknown. In addition, new national security legislation authorizes secret law enforcement activities, some without any reporting requirements.

This lack of openness was the flash point for the Privacy Commissioner of Canada regarding the API/PNR program run by CCRA. According to his 2002 *Annual Report*, when the amendment to the *Customs Act* were before Parliament, he sought and received a formal written undertaking from the CCRA that API/PNR information would be destroyed within 24 hours, except in those relatively few instances where this data identified an individual for secondary screening. Some time later he was told that CCRA had decided to keep all API/PNR information about Canadian travellers for a period of six years in a new database.[64] The federal Privacy Commissioner objected to what he characterized as a clear deception by the Government of Canada.

Lack of openness has lead to a great deal of uneasiness and speculation about the scope of the TIA program. It is known that it will use data retrieval, biometric identification and other technologies to analyze information in databases. What has not been disclosed by DARPA is what databases will be searched. One of the resulting fears is that private purchases and travel patterns will now become subject to government inspection.

In a January 10, 2003, letter to Attorney General Ashcroft, Senators Patrick Leahy, Russell D. Feingold, and Maria Cantwell asked for a clear explanation of the scope of the TIA program. They wanted to determine the extent to which the Justice Department would rely on data mining and what safeguards would be in place for the collection, use and dissemination of information. Specifically, the Senators wanted to know:

- What government, private sector or proprietary databases are being obtained or used by the Department of Justice for data mining or pattern recognition activities?
- Is the Department using any data mining tools to obtain information for law enforcement purposes unrelated to the detection and prosecution of terrorism?

- What procedures, if any, does the Department follow to ensure the accuracy and reliability of information currently collected and stored in databases used for data mining?[65]

One of the provisions in the *USA PATRIOT Act* that received much criticism related to secret searches – these are searches without notifying the subjects until long after the search has been executed. This is a significant change from previous practices. Such notice is considered a "crucial check on the government's power because it forces the authorities to operate in the open and allows the subject of searches to challenge their validity in court."[66]

Another openness concern relates to the reduction in the scope of freedom of information legislation. In both Canada and the United States, there has been a conscious effort by government to limit the public's ability to access information about national security measures.

For example, the *Homeland Security Act* empowers the Department of Homeland Security to withhold information it receives voluntarily from "non-Federal entities or individuals" that relates to "the vulnerability of a critical infrastructure" including computers critical to communication, transportation, and banking. Senator Patrick Leahy called this "the most severe weakening of the *Freedom of Information Act* in its 36-year history." He said it "would hurt and not help our national security, and along the way it would frustrate enforcement of the laws that protect the public's health and safety."[67]

In an effort to fight the erosion of freedom of information Senators Leahy, Levin, Jeffords, Lieberman and Byrd introduced the *Restore Freedom of Information Act* on March 12, 2003. The Bill would clarify and narrow exemptions to the *Freedom of Information Act* (FOIA) created by the *Homeland Security Act of 2002* by:

- Limiting the FOIA exemption to relevant "records" submitted by private entities, so that only those records actually pertain to critical infrastructure safety are protected.
- Removing the restrictions on the government's ability to use the information it receives, except to prohibit disclosure where such information is appropriately exempted under FOIA.
- Protecting the actions of legitimate whistleblowers by removing the unnecessary criminal penalties.
- Respecting, rather than pre-empting, state and local FOIA laws.[68]

Weakening or Elimination Judicial Controls

Many of the anti-terrorism initiatives altered or eliminated traditional checks and balances that function to protect society against abuse from government. This has been one of the most significant areas of concern, particularly in the United States.

The proposed TIPS program would have allowed U.S. federal law enforcement agents to avoid the constitutional requirement of warrants or subpoenas before launching a search or an investigation. This would have been possible because individuals who are not law enforcement officers are not required to get a search warrant in order to look around a home where they are laying carpet, hooking up cable TV or a telephone, or connecting a gas stove.[69] Harvey Silverglate, a Boston civil liberties lawyer, warned: "It's a way into every American's home without judicial oversight."[70]

Previously, the law relating to wiretaps and pen register/trap and trace devices authorized the execution of a court order only within the geographic jurisdiction of the issuing court. The *USA PATRIOT Act* expanded the jurisdictional authority of a court to authorize the installation of a surveillance device anywhere in the United States. In addition this provision is not limited to investigations of suspected terrorist activity.

According to the EFF, the FBI and CIA can now go from phone to phone, computer to computer without demonstrating that each is even being used by a suspect or target of an order. The government may now serve a single wiretap, FISA wiretap or pen/trap order on any person or entity nationwide, regardless of whether that person or entity is named in the order. The government need not make any showing to a court that the particular information or communication to be acquired is relevant to a criminal investigation. In the pen/trap or FISA situations, they do not even have to report where they served the order or what information they received. The EFF believes that the opportunities for abuse of these broad new powers are immense.[71]

In addition, under the *USA PATRIOT Act* the FBI need not show probable cause or even reasonable suspicion of criminal activity. Critics maintain that as a result judicial oversight is now essentially nil.

> With this law we have given sweeping new powers to both domestic law enforcement and international intelligence agencies and have eliminated the checks and balances that previously gave courts the opportunity to ensure that these powers were not abused. Most of these checks and balances were put into place after previous misuse of surveillance powers by these agencies, including the revelation in 1974 that the FBI and foreign intelligence agencies had spied on over 10,000 U.S. citizens, including Martin Luther King.[72]

The reduction of judicial controls also was a point of great concern with Canada's *Anti-terrorism Act*. In its submission to the federal government regarding Bill C-36, the IPC stated:

> The proposed changes to the *National Defence Act* and *Criminal Code* ... would result in a significant reduction of the procedural and judicial controls on electronic surveillance and wiretapping. For example, Bill C-36 reduces the requirement for law enforcement agencies to justify the need for such measures in an application to a judge. There is no longer a need to demonstrate that resorting to a wiretap is the last resort, having exhausted all other investigative techniques. I believe that such justification continues to be necessary in order to ensure proper judicial supervision and oversight.[73]

Lack of Oversight

Along with a reduction in judicial controls, national security legislation removed or lessened other forms of oversight. Under Bill C-36, Canada's Attorney General was empowered to issue a certificate prohibiting the disclosure of certain information. The very existence of the certificate would be secret, and it would not be subject to the *Statutory Instruments Act*. The IPC recommended the certificates, if necessary, be:

- issued by Cabinet, rather than the Attorney General alone;
- subject to review by the federal Information Commissioner and Privacy Commissioner, respectively, as well as the federal court; and
- time-limited.

The IPC also recommended that the CSE be designated as an agency under the *Access to Information Act* and the *Privacy Act* so there could be independent oversight by the Information Commissioner and the Privacy Commissioner, comparable to other law enforcement and intelligence agencies such as CSIS and the RCMP.[74]

Lack of oversight was raised regarding the TIA program in the United States. On November 18, 2002, a "nonpartisan coalition" of over 50 organizations (including the Electronic Privacy Information Center (EPIC), Privacy Rights Clearinghouse, EFF, and the American Civil Liberties Union (ACLU) wrote Senators Tom Daschle and Trent Lott urging them "to stop the development of this unconstitutional system of public surveillance." The letter noted there are "no systems of oversight or accountability contemplated in the TIA project. DARPA itself has resisted lawful requests for information about the program pursuant to the *Freedom of Information Act*."[75]

The broad scope and lack of accountability were the underlying concerns that led the United States Senate to vote to stop all funding for the TIA program until the Pentagon can prove to Congress the program does not violate the privacy rights of Americans. Senator Ron Wyden, who authored the amendment to cut all funding to the TIA, said:

> My concern is the program that has been developed by Mr. Poindexter is going forward without congressional oversight and without clear accountability and guidelines ... That is why I think it is important for the Senate, as we reflect on the need to fight terrorism while balancing the need to protect the rights of our citizens, to emphasize how important it is a program like this be subject to congressional oversight, and that there be clear accountability.[76]

In an effort to address this concern, in February 2003, the Pentagon announced the creation of two boards (one internal and the other an external advisory board) to oversee the TIA program.[77]

Economic Risks

A number of critics believe that the success of electronic commerce in the United States may be threatened by TIA. Wayne Crews, Cato Institute's Director of Technology Policy Studies, thinks the TIA system could undermine electronic commerce because business is predicated on the "sanctity of privately owned databases." He is worried that if companies are forced to submit their databases to inspection by the TIA, "customer's assumptions of privacy would be assailed."[78]

This position was supported by the Association for Computing Machinery (ACM). In a letter to the Senate Committee on Armed Services, the ACM argued that:

> As most non-Americans would oppose allowing the U.S. government access to their personal information, American companies can expect the development of e-commerce systems that exclude the United States, thereby depriving American companies of significant export opportunities. For example, a European Union subsidiary of a U.S. based e-commerce company might be forbidden from running the company's systems in the EU because of the EU's Data Privacy Directive. Alternatively, if privacy restrictions elsewhere in the world conflict with TIA-inspired surveillance, companies may be forced to develop and operate expensive, parallel systems of record-keeping for non-U.S. customers.[79]

Not Effective

Some of the most compelling criticism of the anti-terrorism measures has come from security and technology experts. They have identified a number of troubling technical and methodological problems.

Quite simply, these experts believe that a number of these initiatives will just not work. Regarding the anti-terrorism initiatives introduced in the United States post-9/11, Bruce Schneier, a noted American cryptographer and security expert, wrote:

> A few minutes of speculation should be enough to convince anyone that we cannot make the United States, let alone the world, safe from terrorism. It doesn't matter what Draconian counterterrorism legislation we enact, how many civil liberties we sacrifice, or where we post armed guards. We cannot stop terrorism within a country. We cannot block it at its borders. We have always been at risk, and we always will be.[80]

The greatest concern is that while national security measures will result in pervasive surveillance of the general public, they will not actually enhance security in the process. Operation TIPS was halted primarily for this reason. As one author noted of TIPS:

> Let's be real: Terrorists with half a brain aren't likely to be outsmarted by the mailman or open the door to have the gas meter read if they have bomb-making material nearby.

> But ordinary people, who might be reading the Koran, will. The result could be a flood of unsubstantiated and largely irrelevant tips that overwhelm law-enforcement officials already mired in data. Worst of all, the program could sow the seeds of suspicion among loyal American citizens.[81]

The United States Justice Department maintained it had no intention of recruiting a civilian army of spies. The Department's Director of Public Affairs issued a statement saying Operations TIPS was to be a program that empowered Americans "uniquely well positioned to understand the ordinary course of business in the area they serve, and to identify things that are out of the ordinary."

Given that objective, one critic noted "if the aim is a central database to log suspicious activity, it would be better to simply publish a toll-free phone number for all 285 million Americans, not just 10 million workers with special access to individuals' homes."[82]

Bruce Schneier argues that identity cards would not have stopped the terrorists who attacked the World Trade Center and the Pentagon. According to the FBI, all the hijackers seem to have been who they said they were; their intentions, not their identities, were the issue. Each entered the country with a valid visa, and each had a photo ID in his real name. Regarding the debate about the use of identity cards – smart or otherwise – to enhance national security, Schneier asks: "What problem is being solved here?"[83]

A number of anti-terrorist initiatives in the United States and Canada contemplate matching information collected at points of entry in order to find known or suspected terrorists. For example, in June 2002, the United States' Attorney General John Ashcroft announced a plan to fingerprint and photograph foreign visitors who fall into categories of "elevated national security concern" when they enter the United States. Approximately 100,000 people would be tracked this way in the first year. According to his plan, the fingerprints and photographs would be compared with those of known or suspected terrorists and wanted criminals.[84]

Critics note one of the big problems with such a scheme is no such database of terrorist fingerprints and photographs exists. "Most terrorists are outside the country, and thus hard to fingerprint, and latent fingerprints rarely survive bomb blasts."[85]

The following discussion outlines a number of specific concerns about the effectiveness of anti-terrorism systems (proposed and existing).

Vulnerable and Complicated Technology

Both the Canadian and United States federal governments have talked about using biometric technology such as electronic fingerprinting, face recognition, and retinal scans to confirm identity.

Bruce Schneier agrees that biometrics may be useful in certain circumstances. Face recognition software could be useful to identify authorized airline employees in order to permit them to enter a secure area. But he does not think the technology can pick random terrorists out of the crowd in an airport.

> That much-larger-scale task requires comparing many sets of features with the many other sets of features in a database of people on a "watch list." Identix ... one of the largest face-recognition-technology companies, contends that in independent tests, its FaceIt software has a success rate of 99.32 percent — that is, when the software matches a passenger's face with a face on a list of terrorists, it is mistaken only 0.68 percent of the time. Assume for the moment that this claim is credible; assume, too, that good pictures of suspected terrorists are readily available. About 25 million passengers used Boston's Logan Airport in 2001. Had face-recognition software been used on 25 million faces, it would have wrongly picked out just 0.68 percent of them—but that would have been enough, given the large number of passengers, to flag as many as 170,000 innocent people as terrorists. With almost 500 false alarms a day, the face-recognition system would quickly become something to ignore.[86]

Biometric systems can be poorly implemented and, therefore, can be easily breached. For example, three reporters at *c't*, a German digital-culture magazine, tested a face-recognition system, an iris scanner, and nine fingerprint readers. All proved easy to outsmart.

Smart cards have been routinely breached, often with inexpensive oscilloscope-like devices that detect and interpret the timing and power fluctuations as the chip operates. Another method requires only a bright light, a standard microscope, and duct tape.

Schneier is concerned about building security measures that are so complicated or onerous that they are by-passed. He notes the United States federal government already has several computer networks that are fully encrypted, accessible only from secure rooms and buildings, and never connected to the Internet. Yet despite their lack of Net access, the secure networks have been infected by e-mail viruses. Possibly a staff member checked e-mail on a laptop, got infected, and then plugged the same laptop into the classified network. Secure networks are unavoidably harder to work with and, therefore, people are frequently tempted to by-pass them.[87]

Tempting Target

A number of security experts are concerned about the creation of large national databases that are a component of many of the anti-terrorist initiatives in the United States and Canada.

Currently, government information is scattered through scores of databases, meaning that, however inadvertent, it is compartmentalized so that a breach in one system will not compromise all the data.

The ACM argues immense databases, such as are being proposed by TIA, represent substantial security risks. All-encompassing databases would provide new targets for exploitation and attack by malicious computer users, criminals, and terrorists. The databases proposed by TIA would increase the risk of identity theft by providing a wealth of personal information to anyone accessing the databases. In addition, the ACM thinks it is "unlikely that sufficiently robust databases of the required size and complexity, whether centralized or distributed, can be constructed, financed, and effectively employed in a secure environment, even with significant research advances."[88]

> A single individual who has a personal or political vendetta, or who has been compromised by blackmail or greed, could do great harm. Yet, tens of thousands of systems administrators, domestic law enforcement staff, and intelligence personnel will be able to access the data; the security of the data will depend on the trustworthiness of every one of them. This is not something that can be guaranteed with technology.[89]

The track record for security of government databases is of significant concern to security experts. One American commentator reported that security risks to federal computers and telecommunications systems are worse than ever. Hackers have broken into computer systems of the CIA, Justice Department, National Aeronautics and Space Administration, and the Web page of the Air Force.[90]

> Since September 11 at least forty government networks have been publicly cracked by typographically challenged vandals with names like "CriminalS," "S4t4n1cS0uls," "cr1m3 0rg4n1z4d0," and "Discordian Dodgers." Summing up the problem, a House subcommittee ... awarded federal agencies a collective computer-security grade of F.[91]

Too Much Information

One of the stated objectives of the TIA program is to determine if using technology to predict terrorist attacks is even feasible. Steven Aftergood, the head of the Federation of American Scientists' projects on government secrecy and intelligence, doubts that "technology can be precise enough to distinguish a few suspicious transactions in a sea of activity."[92]

Charles Peña, a policy analyst with the Cato Institute in Washington, said "it's statistically unlikely that the system could predict and pre-empt attacks and also avoid targeting innocent people as suspected terrorists."[93]

> ... if the system – which theoretically would analyze relationships among transactions such as credit card or airline ticket purchases – were applied to the entire population, almost as many people would incorrectly be identified as terror plotters as would be correctly fingered. That scenario would make the technology useless. ...[94]

Security experts do not believe solving national security problems requires a huge electronic infrastructure. In fact, one of the key lessons learned from the September 11 tragedy is that a lack of information was not what prevented the FBI from detecting the terrorists' plans. It was an excess of badly organized and poorly shared data.[95]

> In July, 2001, FBI agent Kenneth Williams warned colleagues in a memo that supporters of Osama bin Laden were attending civil-aviation colleges in Arizona. That important information never made it into the right hands. Six months after two hijacked jetliners brought down the World Trade Center, the Immigration & Naturalization Service sent a letter to the flight school that suspected ringleader Mohammed Atta had attended in Florida, saying his student-visa application had been approved.[96]

Wasted Resources

Some critics believe the scope of a number of the anti-terrorist initiatives will actually result in pulling law enforcement away from critical investigations. This was certainly one of the core concerns about Operation TIPS. Millions of tips could have been filed each week, all of which would have to have been reviewed by law enforcement – wasting valuable resources needed to address real threats to national security.

Easy to Exploit

A *Washington Post* report indicated CAPS used complex computer algorithms, including neural networks, to sort through personal information to identify "suspicious" people.[97] Two students out of the Massachusetts Institute of Technology and Harvard maintain the use of these algorithms actually introduces "a gaping security hole" easily exploitable by terrorists. They argue any security system that uses profiles to select passengers for increased scrutiny is less secure than systems that randomly select passengers for thorough inspection.[98]

In order to understand their arguments, some background information about the operation of CAPS is required. These systems operate according to a two-stage model – profile development, followed by profile evaluation.

Based on a historical record of data pertaining to known terrorist activities, software attempts to detect patterns in the data that "correlate" with prior terrorist plots and "anti-correlate" with the activities of non-criminals. For instance, the software might find that those people who bought one-way tickets using cash and traveled abroad frequently had an elevated chance of being terrorists. Once compiled, this profile is then reviewed by the Department of Justice. Since this process occurs only periodically, "the derived master profile is presumably static for long periods of time."[99]

The approved profile is incorporated into software that is accessible from every airline check-in counter nationwide. When a passenger checks in, the ticket agent enters the passenger's name into the CAPS console. Data mining software linked to government databases searches for information about the passenger, retrieving data relevant to the profile. The software compares the similarity of the acquired data to the profile and computes a "threat index" assessing how much potential risk that passenger may pose. If the passenger has one of the top 3-8% of threat indices relative to the other people on his/her flight, then CAPS flags him/her for "special treatment." A small percentage of people on each flight are randomly flagged as well.[100]

The MIT students present an algorithm called Carnival Booth which they maintain "a terrorist cell can employ to increase their probability of mounting a successful attack under CAPS as opposed to an airport security system that employs only random searches."[101]

A terrorist organization can probe the security system to ascertain which of their members have low CAPS scores. Since security manpower is disproportionately spent on people with high CAPS scores, the terrorist with a low score most likely will face reduced scrutiny.[102] It could be used as follows by a terrorist organization:

- First, probe the system by sending an operative on a flight. The operative has no intent of causing harm. He/she has no explosives or weapons and is simply taking the flight to determine whether or not CAPS flags him/her.
- If flagged, then the organization sends another operative in the same manner.
- Repeat this process until a member who consistently eludes being flagged by CAPS is found.
- Now send this operative on a mission with intent to harm, complete with weapons or explosives. Since CAPS did not flag the operative the last few times, he/she most likely will not be flagged this time and, thus, be subject to less scrutiny.[103]

Newsweek reported in the weeks before September 11, the terrorists practiced their attack by boarding the flights they intended to later hijack (same type of planes, same times, same origins and destinations). They wanted to be certain they did not raise any suspicions or red flags.[104]

The hijackers showed they had no shortage of money, patience, and planning acumen. The terrorists already understood how to use weaknesses in CAPS to their advantage.[105] In conclusion, the MIT students stated:

> The carnival booth effect prevents CAPS from being an effective deterrent against terrorism. ... In short, the financial resources our nation commits to counter-terrorism should not support a CAPS-like system, which may appeal to our intuitions, but is in fact more amenable to compromise.[106]

Solving the Wrong Problem

It is impossible to seal up a country or protect every access point. To illustrate the scope of even contemplating such action, one American noted:

> In 2000, more than 350 million non-U.S. citizens entered the country. In 1999, Americans made 5.2 billion phone calls to locations outside the United States. Federal Express handles nearly five million packages every business day, UPS accounts for 13.6 million, and until it became a portal for terror, the Postal Service processed 680 million pieces of mail a day. More than two billion tons of cargo ran in and out of U.S. ports in 1999, and about 7.5 million North Americans got on and off cruise ships last year.[107]

Bruce Schneier argues most of the security measures contemplated after September 11 will be ineffective. "Worse, their use may make Americans less safe, because many of these tools fail badly ... Meanwhile, simple, effective, ductile measures are being overlooked or even rejected."[108]

Specifically, Schneier suggests the following:

- To forestall attacks, security systems need to be small-scale, redundant, and compartmentalized. Rather than large, sweeping programs, they should be carefully crafted mosaics, each piece aimed at a specific weakness.
- It is seldom necessary to gather large amounts of additional information, because in modern societies people leave wide audit trails. The problem is sifting through the already existing mountain of data. Calls for heavy monitoring and record-keeping are usually a mistake.
- Security systems that depend on keeping secrets tend not to work very well – airport security is such a system. Procedures for screening passengers, for examining luggage, for allowing people on the tarmac, for entering the cockpit, for running the autopilot software – all must be concealed, and all seriously compromise the system if they become known.
- Some efforts are solving the wrong problem and, therefore, deflecting efforts from the real security risks. For example, the United States' federal government and the airlines are spending millions of dollars on systems that screen every passenger to keep knives and weapons out of planes. "But what matters most is keeping dangerous passengers out of airline cockpits, which can be accomplished by reinforcing the door."[109]

Security experts do not believe that massive surveillance resulting in more information being collected is the answer – better use and co-ordination of existing information by law enforcement, better training of key personnel, and a more informed public could have significant impact on security.

> America needs flight-training instructors like the one in Minnesota who alerted the FBI to Zacarias Moussaoui's alleged desire to learn to fly a plane but not to land one. The country needs alert passengers on airplanes, like those who noticed and took down shoe-bomber Robert Reid on American Airlines Flight 63 from Paris.[110]

Schneier maintains that it is "impossible to guard all potential targets, because anything and everything can be subject to attack. Palestinian suicide bombers have shown this by murdering at random the occupants of pool halls and hotel meeting rooms."

> The most important element of any security measure, Schneier argues, is people, not technology – and the people need to be at the scene. Recall the German journalists who fooled the fingerprint readers and iris scanners. None of their tricks would have worked if a reasonably attentive guard had been watching.[111]

As one commentator in the United States said:

> Get over thinking that America can be made safe. Defending a country as big and commercially robust as the United States raises profound, and probably insurmountable, issues of scale. ... When one target is shored up, nimble transnational cells that can turn on a dime simply find new bull's-eyes. Up against those practical realities, homeland security is the national version of the gas mask in the desk drawer—something that lets people feel safer without actually making them so.[112]

Civil Liberties Concerns

There are a number of significant concerns about how anti-terrorism measures adversely impact civil liberties. Objections to some anti-terrorism measures because of violations to civil liberties are amplified by the fact that their ability to enhance national security is questionable. In the discussion below, specific examples illustrate the major civil liberty issues, but these same concerns arise repeatedly across initiatives.

Unconstitutional

Much debate has revolved around the constitutionality of Canada Customs and Revenue Agency's API/PNR system. Three sections of the *Canadian Charter of Rights and Freedoms* (the *Charter*) are at issue:

- section 1 states that the rights and freedoms set out in the *Charter* are subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society;
- section 7 states that everyone has the right to life, liberty and security of the person, and the right not to be deprived of such except in accordance with the principles of fundamental justice; and
- section 8 states that everyone has the right to be secure against unreasonable search or seizure.[113]

In a legal opinion prepared for the Privacy Commissioner of Canada, former federal Deputy Minister of Justice Roger Tassé found:

> The *Canadian Charter of Rights and Freedoms* is intended to foster values recognized as important in Canadian society. These values include the dignity and autonomy of the individual in a free society – values that are balanced against the interests of the state in the administration of government and law enforcement. The actions of the state must be balanced and proportionate in order to limit the infringement of basic rights considered important to Canadians in the least intrusive manner possible. In light of this Charter requirement, and despite a judicial inclination to be deferential to the policy choices made by Parliament, state authority to require the submission of personal information is not absolute. The Charter, through its establishment of legal rights, permits Canadians, to a degree, to control their personal information, including the submission and use of that information to the state. The regime implemented in the form of CCRA's API/PNR Initiative raises serious questions as to whether it is proportional to the legitimate requirements of the state.
>
> ... we are of the opinion, based on our analysis of Supreme Court decisions relating to section 7 of the *Charter of Rights and Freedoms*, that there is a good case to conclude that the collection, use and disclosure of information pursuant to CCRA's API/PNR Initiative does infringe the rights and freedoms of Canadians guaranteed by section 7 of the *Canadian Charter of Rights and Freedoms* and that by reason of its overbreadth, the API/PNR Initiative cannot be demonstrably justified in a free and democratic society, pursuant to section 1 of the *Canadian Charter of Rights and Freedoms*.[114]

A second legal opinion prepared by retired Supreme Court Justice Gérard Vincent La Forest states:

> While individuals may have a diminished expectation of privacy at border crossings, and customs-related searches may not generally require full compliance with the standards required in other circumstances, the seizure and long-term retention of API/PNR information is in my view deserving of some degree of protection for individual privacy. The CCRA's plan makes no provision for such protection. It would trench upon a reasonable expectation of privacy without either prior authorization or any measure of individualized suspicion. Government agencies would have access to detailed, travel-related information of millions of innocent Canadians. In my view this would violate section 8 of the Charter.[115]

In an October 3, 2002, letter to Minister Eleanor Caplan, David Loukidelis, the Information and Privacy Commissioner for British Columbia noted:

> ... In arguing that this unprecedented, open-ended surveillance of Canadian citizens is proportional to the security benefit that is to be derived, you said that the "sort of catastrophe that can be brought about by weapons of mass destruction is without a doubt

justification for keeping this information." This response mocks the concept of proportionality that underpins s. 1 of the "Charter of Rights and Freedoms" and amounts to a bold justification for even more egregious state actions.[116]

Freedom of Speech and Political Association

When introduced, Canada's *Anti-Terrorism Act*, Bill C-36, was severely criticized because it created far-reaching powers with major implications for civil liberties. Of particular concern was the Bill's sweeping definition of terrorism many felt jeopardized freedom of speech and political association. Amnesty International argued the provisions of this definition were "too far-reaching" and included in its ambit activities carried out in full accord with international human rights standards. For example, individuals whom Amnesty International would consider to be "prisoners of conscience" could have been prosecuted under this definition.[117]

The same concern was raised about the *USA PATRIOT Act*. The legislation created a federal crime of "domestic terrorism" that broadly extended to "acts dangerous to human life that are a violation of the criminal laws" if they "appear to be intended ... to influence the policy of a government by intimidation or coercion," and if they "occur primarily within the territorial jurisdiction of the United States."[118]

As this crime is couched in such vague and expansive terms it is feared it may be read by federal law enforcement agencies as permitting the investigation and surveillance of political activists and organizations based on their opposition to government policies. It also could be read by prosecutors as licensing the criminalization of legitimate political dissent.

Vigorous protest activities, by their very nature, could be construed as acts that "appear to be intended ... to influence the policy of a government by intimidation or coercion." Further, clashes between demonstrators and police officers are acts of civil disobedience. Even those that are entirely non-violent could be construed as "dangerous to human life" and in "violation of the criminal laws." Environmental and anti-globalization activists who use direct action to further their political agendas may be particularly vulnerable to prosecution as "domestic terrorists."[119]

Reportedly, the FBI has investigated political dissident groups it claimed are linked to terrorism – among them pacifist groups such as the United States' chapter of Women in Black, which holds peaceful vigils to protest violence in Israel and the Palestinian Territories. As one of the group's members said: "If the FBI cannot or will not distinguish between groups who collude in hatred and terrorism, and peace activists who struggle in the full light of day against all forms of terrorism, we are in serious trouble."[120]

Presumption of Innocence

The principle of the presumption of innocence (i.e., everyone is presumed to be innocent until proven guilty) is embodied in subsection 11(d) of the *Canadian Charter of Rights and Freedoms*.[121] There are concerns that the profiling used in a number of anti-terrorism initiatives will turn this presumption of innocence into the presumption of guilt.

Computer profiling is seen to shift the burden of proof from the government having to prove wrongdoing to data subjects having to prove their innocence. Individuals who fit the profile will be treated differently from those who do not. Guilt is inferred from the probability that an event will or has occurred. A judgment is made about a particular individual based on the past behaviour of other individuals who appear to be statistically similar.[122]

In the United States this concern was raised about the type of profiling used by CAPS. Passengers who "fit the profile" are selected for heightened security measures, which can include a thorough search of their luggage in front of other passengers, intrusive personal questioning, tagging of luggage with orange tape, and a physical escort from the check-in counter to the airport gate by security personnel, in full view of other passengers. The ACLU has long criticized passenger profiling, calling it "a speculative means of predicting criminal conduct that does nothing to insure safety."[123]

Search and Seizure

Supporters of the creation and use of national databases argue that harm to individuals is minimal – most individuals are not even aware of the profiling. They also hold the view that "if you've done nothing wrong, you don't have anything to worry about."

Opponents, on the other hand, view the creation of large scale databases and the use of profiling as nothing more than sanitized search and seizure. They think many of the anti-terrorism systems will amount to a general electronic search, a "fishing expedition" or "dragnet," because the collection, use and disclosure of personal information is done without consent and without any pre-existing evidence or suspicion of wrongdoing.

A traditional law enforcement investigation is generally triggered by some evidence that a person is possibly engaged in wrongdoing. Concerns arise because many of the anti-terrorism measures are not bound by this limitation. They are directed not at an individual, but at an entire category of persons that "fit the profile." They are not initiated because a specific person is suspected of misconduct, but because a category of people is of interest to law enforcement (i.e., those who purchase one-way airline tickets with cash, or those who purchase large quantities of ammonium nitrate, such as Terry L. Nichols who was involved in the Oklahoma City bombing). What makes these anti-terrorism measures fundamentally different from a traditional law enforcement investigation is their very purpose is to generate the evidence of wrongdoing required before an investigation can begin.[124]

Due Process

The issue of due process is one of the most contentious in the ongoing debate about the lawfulness of a number of anti-terrorism measures. Due process refers to the right to view, challenge and refute the government's information before a formal decision is made.

A number of legislative changes authorize law enforcement to delay notice of action or to withhold information from the individual who is the subject of the surveillance. To the extent individuals are denied knowledge and adequate opportunity to challenge or contest the conclusions, they are denied due process of law.

When introduced, one provision of Bill C-36 would have empowered the Solicitor General to recommend groups be put on a public "terrorist" list without any advance notice or an opportunity for response prior to listing. The lack of due process and procedural protections were at the core of the criticism surrounding this provision.

Later amendments incorporated a number of protections including provisions for removal from the list, judicial review and safeguards to address cases of mistaken identity. In addition, the list must be reviewed every two years by the Solicitor General.[125] However, it should be noted that groups may still be put on the terrorist list without being permitted to see the evidence against them – they only have access to a summary prepared by a judge.

The issue of secret searches also raises significant due process issues. As a result of post-9/11 anti-terrorism legislation, both Canada and the United State can lawfully conduct secret searches. The *Anti-Terrorism Act* adds "terrorism offences" to the list of circumstances under the *Criminal Code* in which an Attorney General may delay notifying a person of an interception for up to three years. The *USA PATRIOT Act* authorizes a person's home to be searched without that person being informed a search was ever performed or surveillance devices implanted. The application of this provision is not limited to terrorism investigations, but extends to all criminal investigations, and is not scheduled to expire.

The new "sneak and peek" search provision of the *USA PATRIOT Act* applies where the court "finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse effect."[126] This is seen as a contravention of the "knock and announce" principle, which forms an essential part of the Fourth Amendment's reasonableness inquiry.[127] When notice of a search is delayed, the subject is prevented from pointing out deficiencies in the warrant and from monitoring whether the search is being conducted in accordance with the warrant.[128]

Law enforcement officials maintain that the arguments regarding violations to due process are misleading. They note the right to confront an accuser never applied to the purely investigative stages of a law enforcement activity. In addition, they argue due process is not an issue if after the investigation is completed, individuals are informed of what information was used, how conclusions were arrived at, and have an opportunity to refute the evidence.

Equal Protection

Critics argue the profiling of certain national, ethnic and religious groups is discriminatory action by the government. In particular, computer profiling is seen as a violation of the right of equal protection under the law.

In November 2001, United States Attorney General Ashcroft announced the FBI and other law enforcement personnel would interview more than 5000 men, mostly from the Middle East, who were in the United States on temporary visas. None of these men were suspected of any crime. The interviews were said to be voluntary.[129]

Civil liberties as well as Muslim and Arab-American organizations objected because the investigations amounted to racial profiling and interviews of immigrants who might be subject to deportation cannot be considered voluntary. A number of law enforcement officials also raised concerns – a few local police departments even refused to co-operate.[130]

In March 2002, Ashcroft announced the Justice Department was launching a new investigation of 3000 more non-citizens, mostly young Arab men. This initiative was undertaken despite the fact that just over half of the initial 5000 could be found for the interviews and little, if any, information was learned. The American-Arab Anti-Discrimination Committee was sharply critical of this new effort saying it was an "ineffective method of law enforcement and constituted an unacceptable form of racial profiling."[131]

When the CAPS program was first contemplated in the United States, the "constitutional fragility" of such a system was recognized by the government. As a result, no CAPS profile was to "contain or be based on material of a constitutionally suspect nature."[132]

The United States Federal Aviation Administration maintained its profiling procedures were not discriminatory and insisted CAPS did not target any group based upon race, national origin, or religion.[133] However, in 1997, a newspaper reporter obtained confidential airline security manuals and found they explicitly listed some ethnic associations, with names of Middle Eastern origin, as grounds for suspicion.[134]

Critics of the anti-terrorism measures also contend they actually foster racial discrimination in the population at large. The ACLU was particularly concerned some of the information provided under the proposed Operation TIPS would have come as a result of personal bias or racial profiling. Law enforcement would have had to follow-up on information provided by uninformed citizens who may be prejudiced.[135]

This concern is not without foundation. For months after September 11 2001, Canada's Muslims were subjected to increased harassment and threats. Recorded incidents included assaults, arson, death and bomb threats, vandalism, malicious e-mails, slurs yelled out of passing cars and looks of distrust in shopping centres and city streets. Places of worship were vandalized, individuals were humiliated and abused, and even children were victimized.[136]

By virtue of visual association and ignorance, Sikhs, Jews and others ethnic and religious groups also reported cases of harassment, intimidation, and violence. On September 15, 2001, in Hamilton, Ontario, a Hindu temple was destroyed by fire set by individuals who, according to police, thought it was a mosque. In addition, a man left a disturbing message on the Hamilton Mosque's answering machine saying in retaliation for the World Trade Center attacks he was going to rape five year old Muslim children.[137]

Fair and Public Trial

There are concerns in both the United States and Canada about anti-terrorism legislation significantly eroding an individual's right to have a fair and public trial. Canada's *Anti-Terrorism Act* placed restrictions on this well-established principle by:

- creating a new subsection to the *Criminal Code* waiving the right to remain silent;
- amending the *Criminal Code* regarding the right to a public trial; and
- introducing new subsections to the *Canada Evidence Act* which provide a Federal Court judge, the Attorney General of Canada and the Minister of National Defence the authority to order the non-disclosure of information during any judicial proceeding.[138]

Amnesty International argued these provisions are inconsistent with a number of the fair trial safeguards found in Article 14 of the *International Covenant on Civil and Political Rights*. Canada ratified the Covenant and, therefore, is bound by its provisions.[139]

Privacy Concerns

Before discussing the specific privacy concerns arising from the anti-terrorism initiatives, it is important to understand that privacy is a highly subjective notion.[140] It means different things to different people.

> Privacy is ... a very personal notion. Within socially and culturally defined limits, privacy allows us the freedom to be who and what we are. The very fact that we are able to interact with others as we might like is because our privacy allows us that choice. By embracing privacy, we exercise discretion in deciding how much of our personhood and personality to share with others. We generally feel less vulnerable when we can decide for ourselves how much of our personal sphere they will be allowed to observe or scrutinize.[141]

Both the United Nation's *Declaration of Human Rights* (Article 12) and the *International Covenant of Civil and Political Rights* (Article 17) recognize privacy as a human right. While neither the Canadian nor United States' Constitutions explicitly use the word privacy, it is, nonetheless, considered to be implicit.

United States Justice William O. Douglas described privacy as found within the "penumbra" of the Bill of Rights[142] – where the Bill of Rights, as a whole, is understood to define or indicate where government should not intrude.[143] Canadian Justice La Forest recognized privacy as being:

> ... at the heart of liberty in a modern state ... Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection ... The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state. ... [Also] there is a privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual.[144]

The House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities studied privacy and concluded:

> Canadians view privacy as far more than the right to be left alone, or to control who knows what about us. It is an essential part of the consensus that enables us not only to define what we do in our own space, but also to determine how we interact with others – either with trust, openness and a sense of freedom, or with distrust, fear and a sense of insecurity.[145]

In any discussion of privacy, however, it is important to acknowledge that it is not an absolute right. Sometimes other rights or interests will justifiably prevail. How privacy rights and other societal interests, such as national security, are weighed in the context of a public policy debate, is discussed in the next section of this paper.

It is possible to identify three major components of privacy: property, person, and information. Each of these zones or realms of privacy are important, if not essential, for the well-being of the individual and, ultimately the society. In addition, all are significantly impacted by current and proposed anti-terrorism initiatives.

Territorial Privacy: This relates to limiting or controlling another's entry to one's own personal place. This spatial sense of privacy relates historically, legally, and conceptually to property. There is a physical domain within which a claim to be left in solitude and tranquillity is recognized. Traditionally, no one may enter without permission, except by lawful warrant.

Bodily Privacy: This is also known as "privacy of the person" and relates to the protection of one's physical self against invasion. Privacy of person is an interest in freedom from interference with one's person and from surveillance.[146] This sense of privacy transcends the physical and is aimed essentially at protecting the dignity of the human person. It is protection against the indignity of the search and its invasion of the person in a moral sense. Traditionally, a claim to the privacy of one's person was protected by laws guaranteeing freedom of movement and expression, prohibiting physical assault, and restricting unwarranted search or seizure of the person.

Informational Privacy: This relates to the interest of a person in controlling the information held by others about him/herself. This notion of privacy derives from the assumption that all information about individuals is in a fundamental way their own, for them to communicate or retain as they see fit.[147] The ability to control information about one's self is linked to the dignity of the individual, self-respect, and sense of personhood.[148]

There are relatively few cases where one's privacy can be said to have been breached in the absence of personal information being recorded in some form. Surveillance systems introduced as part of national security initiatives involve the collection, use and disclosure of personal information. Accordingly, the discussion below of the over-arching privacy concerns concentrates on informational privacy issues.

These privacy issues should not be read in isolation. It is precisely because of the ineffectiveness and lack of justification of certain measures, as well as the significant violations of civil liberties, that privacy is such a concern.

It is also important to note that since many of the anti-terrorism initiatives target certain groups, their privacy rights are infringed much more than people who do not fit the "profile."

Big Brother

The scope of government surveillance contemplated under the anti-terrorism initiatives is staggering. National security concerns will drive forward programs like TIA and expand, even further, the degree to which government will be able to monitor and track any individual – not just known or suspected terrorists.

The expanded use of surveillance technology and the creations of new centralized databases, combined with the powerful analytical software to mine and profile, pose significant threats to the privacy of everyone in the United States and Canada.

The public has long feared a single omniscient government database. With TIA, this fear is approaching a reality. Today there is a higher degree of surveillance than ever before. Not only is the scope broader and the application more frequent, but surveillance technology itself is able to probe ever deeper into physical, social, and psychological realms.

Surveillance technology also penetrates "place" and "space," making it virtually impossible to keep things private by locking the door, pulling the shades, erecting a fence, sealing an envelope, or communicating by telephone or e-mail.[149]

Surveillance systems are linked to modern information management systems with massive integrated computer databases and powerful analytical software. Data in diverse forms, from widely separated geographic areas, organizations and time periods easily can be merged and analyzed. Increased

capabilities and decreasing costs permit more and more data to be stored permanently in law enforcement databases. The result is that one's past is always present.[150] As one author noted: "No fact unrecorded, nothing forgotten nor lost, nothing forgiven."[151]

Surveillance technology greatly enhances law enforcement's ability to gather data without the participation or even awareness of the individual. It no longer detects just what someone says or does consciously. Involuntary or autonomic behaviour can now be closely monitored. This type of "biological surveillance" involves technology that collects and analyzes body clues, such as pulse, eye movements, voice, blood, urine, and saliva.

> To be alive ... is to automatically give off signals of constant information – whether in the form of heat, pressure, motion, brain wave, perspiration, cells, sounds, olifacteurs, waste matter, or garbage, as well as more familiar forms such as communication and visible behaviour. These remnants are given new meaning by contemporary surveillance technologies.[152]

It is not just advances in technology that have resulted in greater surveillance – the reduction or elimination of traditional judicial controls (discussed earlier) and a change in focus to prevention rather than detection also contributed to increased use of surveillance technology. There has been a shift from targeting specific suspects to categorical suspicion of groups. Using computers to predict future behaviour and the likelihood of an occurrence has resulting in "anticipatory surveillance" of individuals, groups, and locations.[153] Technology has given law enforcement the ability to seek out violations, even without specific grounds of suspicion.

The proliferation of advanced surveillance and information management technology is a source of concern to the public. People feel vulnerable in the face of the invasive and unrestricted surveillance contemplated by the government, in the name of national security. They are concerned technology will jeopardize or override fundamental human values such as privacy and respect for individuals.

The overarching privacy concern with anti-terrorism initiatives is the extent of the surveillance – that North America will become a society in which unparalleled amounts and specificity of personal information is collected, used and disclosed by governments on a routine and systematic basis.

Loss of Autonomy

The potential loss of personal autonomy resulting from pervasive surveillance is a central privacy concern. Simply stated, autonomy is "the quality or state of being independent, free and self-directing."[154]

Privacy concerns arise because of the potential for individuals to lose control over their personal information. The significance of this concern should not be underestimated. People tend to feel that the loss of control over their personal information has a significant impact on their ability to be autonomous.

> ... not only does the loss of control of information about one's self have some possible serious negative consequences, such as no protection from misuses of the information, it also means a loss of autonomy ... Loss of autonomy means loss of one's capacity to control one's life... A right to control information about one's self is fundamental to being a self-determining and responsible being.[155]

This sentiment was echoed in the report from the 1985 Workshop on Information Technologies and Personal Privacy in Canada:

> The consequences of losing control over personal information go beyond the issue of invasions of privacy. A fundamental aspect of life is being endangered – the freedom to be oneself and the freedom to speak and act. If people think or know that their activities are being monitored or recorded, they tend to act cautiously to protect themselves, and may even start to censor their thoughts and actions. Therefore, the issue of privacy is related to the much larger dimension of personal and political freedom.[156]

Loss of Anonymity

Another disturbing aspect of widespread surveillance is the loss of anonymity. Being anonymous is to be unnamed. As more fragments of one's lives are recorded and stored in databases, people feel their privacy has been invaded, they have lost control over their personal information, and they are, in essence, under surveillance. The creation of an "informational panopticon" such as being contemplated with the TIA program makes people's lives visible to scrutiny by government. It also deprives them of their ability to withdraw themselves from public view.[157]

People desire anonymity for a variety of reasons. Certainly some people may wish to avoid detection from law enforcement in order to undertake unlawful activities. But most people want to have the ability to be anonymous simply because, in North America, it is key to people's sense of freedom and autonomy. It enables the free expression of political ideas, voting without fear of retaliation or coercion, and the practice of religious beliefs without fear of government intimidation.[158]

The courts have upheld the need for a compelling public interest before governments can require individuals to identify themselves. With the elimination of many judicial controls and the introduction of programs such as TIA, CAPPS II and API/PNR, individuals' ability to remain anonymous when they choose has been severely eroded.

Anti-terrorism measures substantially increased the government's ability to invade public and private lives. While surveillance technology is still not at the level where it can identify members of the public in the street, the combining of public and private databases will result in people being identified in ways not previously required. This is seen as an affront to personal dignity and an invasion of privacy. Justice Louis Brandeis' renowned definition of privacy, the "right to be let alone," is under siege.[159]

Loss of anonymity is one of the main reasons people object to identity cards, particularly ones with biometrics. If biometric identifiers are widely used and shared, people's freedom to separate their identity could be restricted. All information about them could be linked, and they will always be identified by their biometric data. Their ability to remain anonymous will be severely diminished.[160]

Lack of Consent and Knowledge

The anti-terrorism initiatives involve the collection, use and disclosure of personal information without the data subject's consent. Rarely would individuals even be aware of when and how they are under surveillance or being profiled.

The cloak of secrecy surrounding the anti-terrorism systems means individuals are not in the position to know what personal information is collected and used. While understanding the need for confidential collection of personal information in the context of law enforcement for certain circumstances, data subjects are not in a position to make informed decisions or to challenge conclusions made about them.

The capability of many of the anti-terrorism systems to compile, combine, and analyze information in a manner never before possible creates another privacy concern. The "ability to assemble information selectively, or to correlate existing information, can be functionally equivalent to the ability to create new information."[161] With systems such as TIA the government can, in essence, create new personal information without the data subject's knowledge or consent.

Most people acknowledge the government needs to collect, use, and disclose some personal information during the course of law enforcement and national security activities. Informational privacy concerns arise when the collection, use and disclosure of personal information becomes so extensive that it crosses the line into pervasive surveillance, with the government using personal information for purposes that go beyond the public's reasonable expectations.

Necessity and Relevance of Personal Information

A central tenet of informational privacy is that the collection of personal information should be limited to data necessary and relevant to a legitimate purpose. One of the primary privacy concerns with the massive computers systems contemplated under a number of the anti-terrorist measures is that more personal information than is necessary and relevant to law enforcement will be collected, used and disclosed.

To do their job effectively, many law enforcement agencies believe they cannot know too much, and they dare not know too little.[162] The development of extensive and integrated databases for national security purposes presents a challenge to the consideration of relevance.

With improvements in information-handling capabilities, comes the tendency to use more data and to discard less. This, in turn, motivates the collection of more data on more variables.[163] Contributing to this tendency is the fact that once a system has been established, the cost of collecting, storing and analyzing additional information is marginal. One of the primary privacy concerns is that, because technology can provide an extremely convenient and cost-effective way to gather and analyze data, more information than is necessary and relevant to a purpose will be collected and used.

Without current information management technology, some data would be inaccessible because the compilation and analysis of the hardcopy information would be administratively burdensome and impractical. The ease with which data can be combined and analyzed with computers means that more information may be used to make decisions with the technology than without it. The notion that more information results in better decision-making seems to prevail. More significantly, it also means that information collected for one purpose may be used for other purposes, generally without the knowledge or consent of the data subject, without an initial assessment of relevancy.

Critics argue there is a need to recognize that the use of more information does not always result in better decisions. They believe limits need to be placed on the collection of personal information, even in the context of national security investigations.

The challenge is to identify data that are truly relevant, and avoid collection for collection's sake or for some unknown future use. This is especially difficult in the context of intelligence work, and the problem has been further compounded by the use of modern surveillance technology.

Some national security measures, at least at this early stage of development, have not been calibrated to filter out irrelevant personal information. The unblinking eye of a video camera, for example, takes in everything, not just that which is related to an investigation.

> There are practical difficulties with a principle that requires record keepers to collect only information relevant to the purpose for which it was collected. How, for example, is relevance to be assessed at the point of collection? ...
>
> In surveillance work, a considerable amount of information about an individual may have to be collected before the relevance of any of it to an investigation is established. Much criminal intelligence work is simply the collection of as much information as possible about known criminals and their associates. Patterns of conduct may then emerge which would not emerge if the only information collected were that obviously relevant at the time of collection.[164]

Given the indiscriminate nature of a number of the anti-terrorism systems, covert surveillance of the general public will become the norm. Many people wonder why it is necessary to put everyone under surveillance, particularly when the effectiveness of that methodology is highly suspect.

Unrelated Use and Disclosure

Another significant privacy concern about the anti-terrorism initiatives is that personal information collected for one purpose will be used and disclosed for unrelated purposes by unrelated parties. The very purpose of these systems is to collect personal information from diverse public and private sector sources, identify patterns and draw conclusions about possible future action – in essence, they are designed to use personal information for purposes for which it was not intended. Even in the context of fighting anti-terrorism, this is considered an invasion of privacy. Going on a vacation does not give the government the right to profile someone and their family.

This issue is of particular concern with regard to identity cards. Once a unique personal identifier has been established, it can be used as a means of collating disparate and dispersed personal data on individuals – from government as well as private sector databases. Such an identifier not only enables individuals to be tracked, perhaps in real time, but creates the potential for the collation of their personal information into a comprehensive profile, unbeknownst to the individuals to whom the data relates.

This fosters concerns that:

- information will be used out of context to the detriment of the data subject;
- unjust decisions about them will be made simply on the basis of a profile;
- automatic decision-making will be based on facts of doubtful completeness, accuracy, relevance, or utility;
- and all of this will be done without the data subject's permission or knowledge.

In its submission to the Standing Committee on Citizenship and Immigration on the issue of a proposed national identity card, the IPC noted:

> Not only would a national ID card be redundant for many of its stated purposes, it could also potentially act as a privacy-eroding tool. The card would likely be supported by a national ID database or linked database registration system. The creation of a national database containing information on all Canadians would be unprecedented and far-reaching. The opportunity for government surveillance and tracking of lawful activities would be significantly expanded.
>
> Undoubtedly, the introduction of a national ID card would be accompanied by government commitments that the use of the card would be strictly limited to specific, identified purposes. However, similar assurances in the past have proven less than robust. The "function creep" associated with Canada's Social Insurance Number is an example of how the use of one form of identification has expanded over time far beyond its original, narrow purpose.[165]

Much of the privacy concern around Bill C-55, the previous version of the *Public Safety Act, 2002*, related to provisions (sections 4.81 and 4.82) in the *Aeronautics Act* that would have given the RCMP and CSIS unrestricted access to the personal information of all Canadian air travellers on flights within Canada as well as on international routes.

The focus of the concern for Privacy Commissioners across Canada was not the primary purpose of the new provisions, which was to enable the RCMP and CSIS to use this passenger information for anti-terrorist "transportation security" and "national security" screening. The Commissioners were concerned because the RCMP would be empowered to use this information to seek out persons wanted on warrants for *Criminal Code* offences having nothing to do with terrorism, transportation security or national security.[166]

When outlining his concerns about Bill C-55, the federal Privacy Commissioner stated:

> While some exceptional measures might be justified as necessary to enhance protection against terrorism, section 4.82 goes far beyond anti-terrorism. Empowering the RCMP to obtain and scan passenger lists in search of anyone subject to an outstanding warrant for any offense punishable by imprisonment of five years or more has no apparent connection to the purported anti-terrorism purpose of Bill C-55. It appears, rather, to be a dramatic expansion of privacy-invasive police powers without explanation or justification as to its necessity.[167]

Similar privacy concerns have arisen because CCRA wants to use personal information in its traveller-surveillance database for unrelated secondary uses. In a joint letter to the Honourable Elinor Caplan, Minister of National Resources, the Privacy Commissioners across Canada stated:

> ... the information contained in the database can be used for purposes unrelated to anti-terrorist security. Rather than collecting and retaining the personal information of a small number of targeted air travellers, as originally planned, the database is far greater in scope and now is slated to expand. We are disturbed that the federal government, in the face of these concerns, plans to expand the databases even further to include personal information on individuals who arrive in Canada by other means, such as trains, ships and buses.[168]

CCRA's reason for creating this database is "forensic." In order words, the Canadian Government wants to be able to use this database to search for relevant information, including known associates, in the event there is a terrorist attack and some of the perpetrators are known. Apparently, it also may want to be able to use this database to identify "everything from routine income tax investigations to trying to flag Canadians as potential pedophiles or money launderers solely on the basis of their travel patterns."[169]

The federal Privacy Commissioner maintains Bill C-17 should be amended to limit police access to "matching air passenger information against anti-terrorism and national security databases."[170]

Data Quality

Another privacy concern about the anti-terrorism systems is the accuracy of the information or lack thereof. Data quality is one of the fair information practices recognized in both Canadian and American privacy legislation.

The issue of accuracy was of particular concern in regard to the proposed TIPS program. According to a 1992 report by Harvard University's Project on Justice, the accuracy of informant reports is questionable, with some informants embellishing the truth and others suspected of fabricating their reports.[171]

The ACM expressed concerns about the potential number of false positives in the TIA program – "in this case incorrectly labeling someone as a potential terrorist." The Association noted that as the entire population of the United States would be subjected to TIA surveillance, even a small percentage of false positives would result in a large number of law-abiding Americans being mistakenly labelled.

> ... suppose the system has an 99.9% accuracy rate. We believe that having only 0.1% of records being misclassified as belonging to potential terrorists would be an unachievable goal in practice. However, if records for everyone in the U.S. were processed monthly, even this unlikely low rate of false positives could result in as many as 3 million citizens being wrongly identified each year. More realistic assumptions about the percentage of false positives would drive the number even higher.[172]

Data quality also is an issue for those anti-terrorism systems utilizing data mining, matching or profiling. Database fields are not standardized, and the data they contain is not always reliable. Names get misspelled, digits are transposed, addresses are outdated or incorrect, and few names are unique.

Some critics are concerned if inaccurate information is used in a profile, such as contemplated under TIA, CAPPS II or API/PNR systems, it may be taken out of context or misapplied. An additional problem relating to the accuracy of information is the fact that computers tend to "freeze dry" information. Data that was accurate for a moment in time may be preserved by a computer and then that moment extended temporally and spatially through a data match or profile, often to the detriment of the data subject.[173]

Privacy versus National Security

In Canada and the United States privacy is recognized as a fundamental, though not absolute, human right. What this means is it does not always have primacy over other rights or values. A number of interests may, depending upon the circumstances, compete with and even take precedence over privacy, including:

- freedom of expression;
- freedom of information;
- protection of economic, trade and state secrets;
- prevention and detection of crime and apprehension of offenders; and
- maintenance of national security and an effective defence capacity.[174]

In a September 21, 2001 statement about the terrorist attacks in the United States, the IPC noted that since privacy is not an absolute right, there are circumstances when privacy has given way to legitimate law enforcement and public safety concerns.[175]

In an effort to reconcile these competing interests, a balancing model has developed. In the public policy debate about anti-terrorism initiatives, the individual's right to privacy has been balanced against the need to protect the country from terrorist attacks.

The balancing model pits public interest against the individual's interest. In the debate surrounding anti-terrorism initiatives, a tension has been created between self-interest (i.e., privacy and freedom from government surveillance), and public interest (i.e., national security).

The traditional view of privacy is that it is fundamentally about the power of the individual. It allows individuals the freedom to be who and what they are. Priscilla Regan believes this view fails to recognize the broader social importance of privacy.

> Privacy is a *common value* in that all individuals value some degree of privacy and have some common perceptions about privacy. Privacy is also a *public value* in that it has value not just to the individual as an individual or to all individuals in common but also to the democratic political system. The third basis for the social importance of privacy is derived from the theoretical literature in economics. Privacy is rapidly becoming a *collective value* in that technology and market forces are making it hard for any one person to have privacy without all persons having a similar minimum level of privacy.[176]

By narrowly defining privacy as a right of the individual alone, the basis for its protection is weakened. The protection of privacy is dependent upon the power of the individual. One of the significant dangers in the balancing process is balances are "all too easily struck at a certain level, so

that privacy is traded off in concessions to managing surveillance, rather than restricting it."[177] Too often, then, privacy is sacrificed for what supporters of the anti-terrorism measures argue is the greater good.

In order to ensure privacy is given its due in the public policy debate about national security, it is important to understand that the idea of balancing individual rights against the public interest is "a false model, and the problem is in the metaphor."[178] The implicit assumption of the balancing model – that a right can always be balanced against other interests – is incorrect. Such logic would mean that in any given instance, the claim to the right of privacy might be disallowed.[179]

When a right is balanced against a desired outcome (e.g., a safe and secure society) the protection of that right can become very situational. Also, the balancing model encourages comparative thinking about the goals and means. The more important the goal (e.g., national security), the greater the acceptance of means that are less than ideal. This model makes it easier to justify violating an individual right when the goal serves the community or the country.[180] In other words, the end justifies the means.

Gary Marx noted the "ethical acceptability of means" is often "contingent on ends." If the intent is "noble, then the action is justified, even if it has some bad effects."[181] In a post-9/11 world, to what degree does national security have to be enhanced to make wide scale surveillance acceptable? So far, just the promise of enhancement seems to be justification enough for the Canadian and American governments.

While the idea of balancing private interests versus public interest may be appealing in its simplicity, it implies that privacy can be disregarded or eliminated when there are overriding societal interests. This is not the case. As Alan Westin noted, if all that was needed to win legal and social approval for surveillance was to point to a social problem and show that surveillance would help to cope with it, "then there is no balancing at all, but only a qualifying procedure for a license to invade privacy."[182]

New model

Advances in surveillance and data mining technology, and the promise of more to come, have stripped away traditional physical and administrative barriers that previously protected privacy. In addition, in the name of fighting terrorism, judicial controls and protections under freedom of information and privacy legislation have been aggressively reduced by the Canadian and United States governments.

There is a tendency to simplify the balancing model to where an individual's privacy is at one end of a scale, and public safety and national security is at the other – when one is up, the other is down. Societal concerns and privacy values are seen as antithetical.[183]

Privacy's value is both public and private. Privacy is an instrumental good, having value not only as an end in itself but as a means of achieving other ends.[184] As one writer observed, "in one sense, all human rights are aspects of the right to privacy."[185] Privacy plays an enabling role in other human rights such as freedom of association and freedom of speech. Some claim that it has become "one of the most important human rights issues of the modern age."[186]

The public value of privacy derives not only from its protection of the individual as an individual, but also from its usefulness as a restraint on the power of the government. "Privacy in this sense is not important just to individual liberty but also to civil or social liberty because it helps establish the boundaries for the exercise of power".[187]

This view is supported in a number of American Fourth Amendment cases on the prohibition of unreasonable search and seizures. The public value of privacy is "derived from its importance to the exercise of rights that are regarded as essential to democracy, such as freedom of speech and association, and from its importance as a restraint on the arbitrary power of government."[188]

However, Priscilla Regan thinks if the public value of privacy is reduced to just due process protections, its "completeness" may be overlooked. She looks to Hannah Arndt's discussion of the public and private realms to identify "an independent public value for privacy."[189]

In order for the "common" to develop in the public realm, the private realm is essential. In other words, in order for Canadians and Americans to view themselves as part of their community and country, privacy must exist. "If the private realm is destroyed, the public is destroyed as well because the human is destroyed."[190]

Regan also argues privacy is key to the development of trust and accountability which are necessary components of a democratic society. Privacy violations negatively impact people's ability to function publicly as part of that society. Oscar Gandy also makes this point: "The same technology that threatens the autonomy of the individual seems destined to frustrate attempts to reestablish community and shared responsibility because it destroys the essential components of trust and accountability."[191]

The argument "if you have nothing to hide, you have nothing to fear," which is often put forth by supporters of surveillance, is based on faulty analysis of the issue. The harm, of course, is in the change in the level of social control.[192] Pervasive surveillance of the population will in time, harm the innocent. The level of distrust that manifests itself when people live, over time, under constant surveillance erodes the foundation of a democratic society.

Thus it is critical that the importance of privacy both to the individual, as well as to the society as a whole, be recognized. Privacy is not repealed or abolished simply because governments want or need to advance an objective – regardless of its social importance.

A new way of understanding the enduring importance of privacy and the need for its ongoing protection must be found in the post-9/11 world. Something more than a stated goal of combating terrorism is necessary to justify widespread surveillance and the state's incursions into people's private lives.

Minimize Impact on Privacy

The win/lose zero-sum game equation of the balancing model poses a major threat for privacy because the public's desire for safety will never diminish. When national security is in the balance, privacy will always be seen as expendable. Using this model when developing public policy relating to national security has resulted in widespread surveillance of innocent people being deemed acceptable because of the positive social goal of combating terrorism. Therefore, the model must be re-cast.

Potentially privacy invasive technologies, such as biometrics, electronic surveillance, data mining, and various types of imaging and sensing technology, need to be designed and utilized in a manner that enables them to serve as effective security tools in the fight against terrorism, but also minimizes their impact on privacy.

In June 2002, the IPC issued a paper entitled *Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift*, which argued there is no inherent reason why greater public safety and national security must come at the expense of privacy. Some security technologies can be redesigned to remain highly effective, while at the same time, minimizing or eliminating its privacy invasive features. The STEPs paper issued a a challenge to public policy makers and technologists to move the debate on security and privacy beyond the traditional either/or viewpoint, and to actively seek out opportunities when privacy safeguards can be designed into the framework of national security technology and systems.[193]

Greater safety and security does not always have to come at the expense of privacy. Integrating considerations for privacy and security into surveillance technology is challenging, but not impossible. It is recognized that this may not be possible in all circumstances or with all types of surveillance technology. But some security technology can be redesigned to remain highly effective, while at the same time minimize privacy invasive features.

For example, passenger-scanning technologies are commonplace at all airports and are deployed to identify possible security threats. Such scanning technology has great potential to intrude on the physical privacy of the individuals being scanned. Body scanners display everything under a person's clothing, including concealed weapons, chemicals, restricted objects and the body itself. But there is no security need for the equipment operators to view the essentially naked bodies of passengers. Equally effective but much less privacy intrusive technology exits.

Researchers at the United States Department of Energy have developed a new technology that augments security scanning while addressing this privacy concern. The Department's Pacific Northwest National Laboratory produced a scanning technology using 3-D holographic imaging that focuses on revealing objects hidden underneath the clothing of airline passengers, instead of displaying the entire body. In addition to metal weapons, those made of plastic and ceramics can be detected by the Personal Security Scanner, offering a distinct advantage over systems that rely on metal detectors alone.

Concerns that the unclothed physical features of a person being scanned might be visible to the scanner operator were addressed by reprogramming the system to give operators a view of concealed items only and not the person's image. The Personal Security Scanner is an excellent example of technology designed and deployed in a manner that addresses security requirements while minimizing the invasion of privacy.[194]

By designing privacy safeguards into the framework of national security technology and systems to the extent possible, public safety can be achieved without creating the tools and conditions that permit unchecked data mining and indiscriminate surveillance. This task will not be easy, but consider the alternative. It would be a tragic irony if Canadians and Americans had to give up their rights and freedoms in an effort to secure them.[195]

Below is a discussion of factors that must be considered by government when evaluating surveillance measures and determining how to implement technology and systems in a manner that minimizes the negative impact on privacy.

Justification

Before government uses a potentially intrusive surveillance technology or system, a case must be made as to why it is truly necessary to fight terrorism. What has been missing since 9/11 is a full explanation of why previously existing surveillance and investigative tools are insufficient to combat terrorism.

Merely pointing to the fact of the September 11 terrorist attacks is not justification enough. The burden of proof lies with government and law enforcement to justify their intrusion, not on the individual or the group to show why their right to freedom from surveillance is entitled to protection.[196]

To determine if there is sufficient justification for an invasion of privacy, government should undertake a three-tiered assessment relating to:

- the legitimacy of the goal or its purpose;
- the ability of the proposed technology to appropriately achieve that goal; and
- the potential impact on privacy that both the goal and technology may have.

An examination of the legitimacy of the goal is critical to ensure there is a real and pressing social problem to be addressed. Without this assessment, anti-terrorism measures just become "improved means to an unimproved end."[197] It is also important to assess the urgency of the problem. Inconvenience is not a determining factor in invading someone's privacy. Due to the highly intrusive nature of the surveillance technology used by law enforcement, the Supreme Court of Canada recognized the need for this type of justification in what it called an "investigative necessity requirement."

> The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning.[198]

Certainly no one would dispute that national security is a legitimate and urgent goal. But it can be so broadly defined as to be used as justification for absolutely any state intrusion. In order to be meaningful, public policy goals need to be specific, with demonstrable benefits.

The next area for consideration is the surveillance technology or system being proposed to achieve the goal. In assessing the appropriateness of technology or system, government should consider:

- the seriousness of crime;
- if non-intrusive or less privacy intrusive means are unavailable or ineffective;
- if it can be demonstrated the technology is reliable and effective;
- if there are reasonable grounds to conclude the technology will achieve the goal;
- authorization has been subject to democratic decision-making, however indirect;
- appropriate legislative, administrative and technical policies and controls are in place to ensure the technology, and resulting personal information, will only be used for its intended purposes; and
- there are adequate provision for human vigilance and discretion.

The greater the number and strength of affirmative responses, the more defensible a use of the technology becomes.[199]

Government also needs to consider if the proposed system or technology is proportional to the problem. Is the size, scope, and capabilities of the technology or information system appropriate to the nature of the problem it intends to address, or are the capabilities of the technology or system far beyond the objective need?[200]

The third factor in assessing the justification for surveillance systems is the potential impact it may have on privacy. Obviously, in cases where minutes count in order to protect public safety, an assessment of this kind is not possible. However, a number of the anti-terrorism initiatives, particularly the TIA project, involve the long-term research and development of technology. Here, a process known as a Privacy Impact Assessment (PIA) should be utilized to identify and evaluate the privacy implications of systems and technologies prior to implementation.

One of the important reasons for undertaking this type of assessment is to identify the secondary or even tertiary consequences of technology, rather than just the primary or intended effects. Focusing on the question of what else may happen when surveillance technology is introduced is critical because, in the long run, the unintended and indirect effects may be most significant. Moreover, the undesirable secondary consequences often are unnecessary and may be prevented by proper planning.[201]

The advantages of using a PIA in the context of determining justification for surveillance technology are that it:

- enhances privacy awareness in decision-making and systems design;
- enables government to anticipate the public's privacy concerns;
- allows for consideration of privacy issues in advance of privacy erosion rather than after the fact;
- ensures that privacy risks are identified and properly addressed prior to implementation;
- may identify privacy issues not covered by privacy legislation; and
- could enhance consistency in assessment and regulation of practices and technology that may affect privacy.

The ultimate objective is to enable government and law enforcement to make informed choices and to "opt for a more privacy friendly, but equally effective alternative."[202]

By requiring a justification of anti-terrorism initiatives and raising legitimate privacy concerns, the purpose is not to diminish the ineffectiveness of national security measures. Rather, the purpose is to ensure that the measures are indeed necessary, while protecting privacy to the maximum extent possible.

Effectiveness

Privacy advocates do not fail to understand that national security is a priority for Canadians and Americans.[203] They do not fail to understand there may be a legitimate need to increase surveillance or the investigative powers of law enforcement in order to address threats to public safety. What they want is to ensure that the need for anti-terrorism measures is real and truly effective – otherwise any reduction in privacy is unacceptable. The security gained must be real and not illusory.

It is understandable why the governments of democratic countries around the world responded as they did after the terrorist attacks in the United States. It was an extremely frightening time when the level of anxiety and fear amongst the general populace demanded decisive action on the part of government.

However, upon reflection, it is clear the effectiveness of a number of anti-terrorist measures is questionable. What then can be the justification for subjecting millions of innocent people to these privacy invasive measures when they will not enhance national security?

Anti-terrorism initiatives should be approved by government only if it can be demonstrated how they will effectively address the stated problem. In addition, there should be a process for testing and evaluating the effectiveness of the system or technology over time. If a system is not effective is must not be used. The cost to privacy and other human rights is too great to permit surveillance where no enhancement to national security will result. It is also a waste of valuable time, money and resources that could be utilized to fight terrorism in meaningful ways.

As the Privacy Commissioner of Canada noted in his lawful access submission, there may be at times a need for some new privacy-invasive measures to enhance security and allow law enforcement agencies to investigate crimes and threats to public safety. He suggested any such proposed measure must meet a four-part test:

- it must be demonstrably necessary in order to meet some specific need;
- it must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer;
- the intrusion on privacy must be proportional to the security benefit to be derived; and
- it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.[204]

Limiting Purposes

It is critical to ensure that personal information collected by new surveillance systems is used only for the purpose of national security and not for other unrelated purposes. The enormous capacity to collect personal information of doubtful relevance to national security purposes was one of the central criticisms of a number of anti-terrorism initiatives.

Defining the purpose for which personal information is to be collected, used, and disclosed is the lynchpin for fair information practices embodied in privacy legislation around the world. At the core of this principle is the idea that if the government cannot clearly establish why it needs personal information to fulfill an identified purpose, it should not collect it.

Collection of personal information without justification is never considered appropriate in terms of privacy. Accordingly, controls should be incorporated into the design of anti-terrorism systems to ensure irrelevant personal information will not be collected or used.[205]

When information can be collected selectively, the determination of relevance should be done at that time. However, some surveillance technologies make this distinction practically impossible. Accordingly, the relevance test moves to the time of use.

The ability to identify what personal information is needed to fulfill the identified purpose is much easier to do in the context of a specific investigation than it is in the context of intelligence gathering, which is at the heart of many anti-terrorism initiatives.

> With respect to the scope of intelligence record keeping in general, it is important to remember that the subjects of such surveillance may be individuals who have never been convicted, or indeed accused, of any criminal act. Moreover, the names of persons who have merely had innocent contact with subjects of surveillance may appear in intelligence files and in the computerized name file. The broad range of potential sources of such information and the unverifiable nature of some of the information which may find its way into the system gives rise to classic informational privacy problems and suggests that the scope of such surveillance should be carefully limited to cases where a clear need for it can be demonstrated.[206]

The goal of national security is important, but it does not give government and law enforcement *carte blanche* to collect and use any and all personal information in any way they want. Efforts must be made to define limited purposes and the minimum amount of personal information necessary to fulfil them – even for intelligence gathering. If a reasonable justification cannot be found, agencies should not collect the data. This idea is a cornerstone of the constitutional limits placed on the ability of the state to intrude on the individual.

It is possible to design a relevancy test into some types of surveillance.[207] Voice recognition technology, for example, can free law enforcement from the most labour-intensive aspects of monitoring all parties to a conversation.[208] Another area where technology may actually help in the determination of relevance is e-mail:

> Whether law enforcement accesses e-mail from the telephone company (or access provider) while in transmission, or from an e-mail service provider while it is in storage incident to transmission, it may be relatively easy for the service provider to perform the minimization. The service provider can use screens and filters to select from the e-mail messages to or from

parties identified in the [court] order only those containing certain key words or phrases ... As the investigation proceeds and law enforcement learns more about the patterns of the target, the interception can become more discriminating.[209]

Accountability

Kenneth Laudon identified three types of accountability in his analysis of the FBI's national computerized criminal history systems: technical, legal, and political. Technical accountability refers to the extent to which the flow of information in a system can be accounted for (e.g., ensuring there are proper procedural and technical controls on the collection, use and disclosure of data, and there are appropriate audit trails and reviews).

Legal accountability is the extent to which operators and users of systems can be held legally accountable for the information they collect, use and disclose. Laudon argues systems can be thought of as legally accountable if it is possible to establish responsibility and liability through the actions of systems; if clients of systems have legal standing to sue for damages; and if there is a reasonable probability clients of systems can know that a record-keeping transaction actually harmed them.

Laudon thinks systems can be thought of as politically accountable when they operate under statutory authority and within statutory guidelines; when there is effective oversight, audit and monitoring; and when such systems can be said to be open.[210]

While all three types of accountability are critical, it was the lack of political or public accountability that was the major concern about the anti-terrorism initiatives introduced in Canada and the United States after the September 11 terrorist attacks. Criticism focussed on the lack of openness in the legislative process, as well as the lack of reporting and oversight mechanisms.

Public accountability is important because it ensures that the actions of national security and law enforcement agencies are subject to the proper controls.[211] Quite simple, public accountability is essential to prevent abuse (inadvertent or deliberate) and to protect privacy and civil liberties. It also ensures:

- organized groups can participate in, understand, and oversee the operation of these systems, thereby holding them accountable;
- operators and users of the technology and information systems can be held accountable for the information they collect, use and disclose; and
- a public account can be given of the flow of information in these large information systems.[212]

Effective legislative oversight is one critical component to public accountability. In addition, appropriate judicial controls are essential so the implementation of surveillance technology and other measures designed to combat terrorism may be monitored. Oversight by the courts ensures

any restriction or reduction in the fundamental right to privacy is only permitted when there is a demonstrated prevailing general interest.

> Each interference with privacy must be proportional. Moreover the court stresses the need for organizational and procedural precautions to guarantee the fundamental right. ... the operators have to prove the need to interfere with the people's right. The more one measure interferes with rights, the stricter are the conditions for a justification.[213]

Accountability requires public participation, debate and reporting. It needs transparency in capacity (if possible) and process, as well as appropriate legislative and judicial controls.[214] Some may argue transparency weakens national security efforts – that it just provides more information to the enemy. However, a meaningful distinction may be made between disclosure of detailed specifications of a surveillance system that would enable someone to disable or by-pass it, and disclosure (in the form of an informed public debate) of the:

- need for the surveillance system;
- alternatives examined and why they are inadequate to achieve a defined objective; and
- reasons why the recommended system is appropriate, proportional and effective.

True public accountability requires awareness on the part of the public of the nature and consequences of the surveillance systems introduced as part of governments' national security initiatives.[215]

Accountability also may be enhanced by ensuring that government surveillance systems function within the purview of freedom of information and protection of privacy legislation. These statutes already have exemptions relating to national security, law enforcement and public safety, thereby recognizing such critical information needs to remain secure and confidential in certain circumstances.

Both the Canadian and United States governments have taken steps to reduce the scope of this legislation. In Canada, the independent oversight provided by the Information and Privacy Commissioners has also been eliminated in some instances. Such action has also reduced individuals' ability to access information. The public's right of access is essential to the preservation of democracy as it helps to ensure accountable government.

In addition, having national security initiatives subject to privacy legislation ensures that personal information collected, used and disclosed in the context of anti-terrorism measures is handled in a manner that protects privacy to the greatest extent possible. Privacy legislation defines a set of responsible information management practices with which government organizations, including law enforcement, need to comply.

Public debate, legislative and judicial controls, and other means for ensuring public accountability are critical components in the determination of social justification and acceptability of surveillance technology and other measures designed to combat terrorism.

Conclusion

The very nature of surveillance technologies used by national security and law enforcement agencies is privacy intrusive. To argue such technology should not be used because it invades privacy is not realistic, nor does it acknowledge the very real threats to national security faced by Canada and the United States. Fear of a repeat of the 9/11 attacks and the public's desire for personal safety and national security will continue to drive the policy agenda forward.

However, cautionary voices have been raised in an attempt to slow down what is perceived as unrestricted and unnecessary violations of civil liberties and privacy rights in the name of enhanced national security. More frequently, people are questioning the type of society they want to live in. Secure – yes. Without the protection of constitutional rights and privacy – no.

Privacy is a fundamental human right and must be protected as such. It represents something much more than just a right or interest of the individual. Hungary's Data Protection Commissioner observed that: "One way or another, the health of informational freedom rights always reflects the state of society."[216]

Protection from government surveillance is an area of privacy that helps define the fundamental relationship between individuals and the state. Alan Westin stated, "no society with a reputation for providing liberty in its own time failed to provide limits on the surveillance power of authorities."[217]

Governments must recognize that privacy rights should not be abrogated because the need to catch terrorists is critical. This necessitates an understanding by government that it bears an ongoing responsibility to protect privacy rights to the maximum extent possible, regardless of other interests. Activities ostensibly designed to enhance national security may override or invade an individual's privacy, but the right to privacy continues. It cannot be traded away.

While privacy is not an absolute right, neither are the needs of law enforcement. The balancing model used to weigh competing rights and interests implies that privacy is eliminated or diminished when there are overriding societal issues. This is not the case. Privacy continues to exist and must be protected to the extent possible. All privacy interests are not abrogated in the name of national security.

We maintain that in order for privacy to be given its proper consideration in the public policy debate about national security, government, technologists and, indeed, privacy advocates and Commissioners, must abandon the zero sum paradigm. Security and privacy needs to be viewed as interdependent – not opposing forces. Both are essential ingredients to a free and democratic society.

Pervasive surveillance of the general public is not the antidote to terrorism. Nor is the violation of our fundamental freedoms and rights. The late Justice Thurgood Marshall, United States Supreme Court, observed: "when we allow fundamental freedoms to be sacrificed in the name of real or perceived emergency, we invariably regret it." He also noted: "History teaches that grave threats to liberty often come in times of urgency, when constitutional rights seem too extravagant to endure."[218]

In addition to looking for ways to design privacy-protective measures into surveillance technology, proper justification, legislative and judicial controls, public awareness and accountability are all necessary to ensure that effective anti-terrorism measures may be implemented in a manner that minimizes invasions of privacy as much as possible. This is the challenge that now faces governments in Canada and the United States – they must not fail.

Notes

1. E-mail from Pierrôt Péladeau to the National Privacy Coalition, February 4, 2003.

2. Electronic Frontier Foundation, *Analysis of the Provisions of the USA Patriot Act – That Relate to Online Activities*, October 31, 2001, <www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html>, 01/22/03.

3. Ibid.

4. Center for Democracy and Technology, *CDT Policy Post*, Volume 7, Number 11, October 26, 2001, <www.cdt.org/publications/pp_7.11.shtml>, 01/29/03.

5. Ritt Goldstein, "US planning to recruit one in 24 Americans as citizen spies," *The Sydney Morning Herald*, July 15 2002, <www.smh.com.au/articles/2002/07/14/1026185141232.html>, 01/22/03.

6. Citizen Corp, *Operation TIPS – Terrorism Information and Prevention System*, <www.citizencorps.gov/tips.html>, 07/19/02.

7. Ellen Sorokin, "Planned volunteer-informant corps elicits '1984' fears," *The Washington Times*, July 16, 2002, <www.washtimes.com/national/20020716-75882632.htm>, 01/22/03.

8. Center for Democracy and Technology, *The New Homeland Security Department - Challenge, Potential and Risk – Privacy Guidelines, Careful Oversight Required*, <www.cdt.org/security/homelandsecuritydept/021210cdt.shtml>, 01/21/03.

9. Ibid.

10. The Defense Advanced Research Projects Agency (DARPA) is the Pentagon's main research and development unit.

11. Information Awareness Office, Defense Advanced Research Projects Agency, *Total Information Awareness (TIA) System*, <www.darpa.mil/iao/TIASystems.htm>, 01/23/03.

12. Defense Advance Research Projects Agency, *Defense Advanced Research Projects Agency's Information Awareness Office and Total Information Awareness Project*, <www.darpa.mil/iao/iaotia.pdf>, 01/23/03.

13. Gene Healy, Cato Institute, "Beware of Total Information Awareness," January 20, 2003, <www.cato.org/dailys/01-20-03.html>, 01/29/03.

14. Shane Harris, "Tech Insider: Total information unawareness," *Government Executive Magazine*, November 20, 2002, <www.govexec.com/dailyfed/1102/112002ti.htm>, 01/23/03.

15. Ibid.

16. Electronic Privacy Information Center, "Introduction," *Total Information Awareness (TIA)*, <www.epic.org/privacy/profiling/tia>, 02/04/03.

17. Jim Puzzanghera, "Massive database dragnet explored: Anti-Terrorism Project Alarms Privacy Advocates," *The Mercury News*, November 20, 2002, <www.siliconvalley.com/mld/siliconvalley/4569587.htm>, 01/23/03.

18. Electronic Privacy Information Center, "Introduction," *Total Information Awareness (TIA)*.

19. "Nearly a total invasion of privacy," The Oregonian, February 15, 2003, as cited by the Institute for the Study of Privacy Issues, ISPI Clips 57.306, February 17, 2003.

20. Susan Cornwell, "Senate Blocks Funding for Pentagon Database," *Washington Post*, January 23, 2003, <www.washingtonpost.com/ac2/wp-dyn/A34837-2003Jan23?language=printer>, 01/29/03.

21. United States Department of Transportation, "Airport Activity Statistics of Certificated Air Carriers: Summary Tables," 2001, as cited in Samidh Chakrabarti and Aaron Strauss, *Carnival Booth: An Algorithm for Defeating the Computer-Assisted Passenger Screening System, Law and Ethics on the Electronic Frontier*, MIT/Harvard Law School Student paper, May 16, 2002, <swissnet.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm>, 01/23/03.

22. Center for Defense Information, *CDI Fact Sheet: Transportation Security Agency (TSA)*, January 21, 2003, <www.cdi.org/terrorism/tsa.cfm>, 01/24/03

23. Michigan Advisory Committee, *Civil Rights Issues Facing Arab Americans in Michigan: A Report to the U.S. Commission on Civil Rights*, Chapter 6, May 2001, <www.usccr.gov/pubs/misac2/ch6.htm>, 01/23/03.

24. Ibid.

25. Bret Kidd, "Taking Aviation Security to the Next Level," *EDS Global Transportation Industry Group*, <www.eds.com/about_eds/homepage/home_page_aviation_kidd.shtml>, 02/12/03.

26. William Matthews, "TSA System would dig up passenger info: Privacy advocates warn of 'extensive profiling' by agency," *Federal Computer Week*, September 2, 2002, <www.fcw.com/fcw/articles/2002/0902/news-capps-09-02-02.asp>, 02/12/03.

27. Kidd, "Taking Aviation Security to the Next Level."

28. Robert O'Harrow Jr., "Air Security Focusing on Flier Screening Complex Profiling Network Months Behind Schedule," *Washington Post*, September 4, 2002, p. A01, <www.washingtonpost.

com/ac2/wp-dyn?pagename=article&node=&contentId=A34738-2002Sep3&notFound=true>, 01/24/03.

29. Ibid.

30. "Delta to Test New Airport Security Plan," *Christian Broadcast Network*, February 28, 2003, <www.cbn.com/CBNNews/wire/030228b.asp>, 03/03/03.

31. "Comments Of Senator Patrick Leahy, Ranking Democratic Member, Senate Judiciary Committee, On The Justice Department's Secrecy In Drafting A Sequel To The USA PATRIOT Act," February 10, 2003, <www.senate.gov/%7Eleahy/press/200302/021003.html>, 03/19/03.

32. OMB Watcher, "Patriot Act II Also Limits the Public's Right-to-Know," February 10, 2003, Vol. 4 No. 3, <www.ombwatch.org/article/articleview/1324/1/163/>, 03/03/03, and "PATRIOT Act II?," February 12, 2003, <www.privacyactivism.org/Item/62>, 03/03/03.

33. Department of Justice, *Backgrounder, Royal Assent of Bill C-36 The Anti-Terrorism Act,* December 18, 2001, <canada.justice.gc.ca/en/news/nr/2001/doc_28217.html>, 02/11/03.

34. Department of Justice, "Anti-Terrorism Act Receives Royal Assent," *News Release*, December 18, 2001, <canada.justice.gc.ca/en/news/nr/2001/doc_28215.html>, 02/11/03.

35. Citizenship and Immigration Canada, *Fact Sheet, Citizenship And Immigration, September 11, 2001: A Year Later*, <www.cic.gc.ca/english/pub/sept11.html>, 01/24/03.

36. Air Transat, *Advance Passenger Information System (APIS)*, <www.airtransat.com/en/4_14.asp>, 01/24/03.

37. Canadian Tourism Commission, *Advance Passenger Information (API)/Passenger Name Record (PNR) System Fact Sheet*, No. 2002-05, 05/11/2002, <http://ftp.canadatourism.com/ctxUploads/en_publications/Fact_Sheets_2002-05.pdf>, 01/24/03.

38. Ibid.

39. Oliver Moore, "Privacy czar slams federal plan to track citizens," *Globe and Mail*, September 26, 2002, <www.globeandmail.com/servlet/ArticleNews/front/RTGAM/20020926/wpriv926/Front/homeBN/breakingnews>, 01/24/03.

40. Privacy Commissioner of Canada, News Release, April 9, 2003, <www.privcom.gc.ca/media/nr-c/2003/02_05_b_030408_e.asp>, 04/09/03.

41. Government of Canada, "Government of Canada Introduces Improved Public Safety Act, 2002," *News Release*, October 31, 2002, <www.tc.gc.ca/mediaroom/includes/GOC_printable_release.asp?lang=en>, 01/24/03.

42. Transport Canada, *Backgrounder – Highlights of the Public Safety Act, 2002*, April 2002, <www.tc.gc.ca/mediaroom/backgrounders/b02_gc001e.htm>, 02/13/03.

43. Government of Canada, "Government of Canada Introduces Improved Public Safety Act, 2002," *News Release*, October 31, 2002, <www.tc.gc.ca/mediaroom/includes/GOC_printable_release.asp?lang=en>, 01/24/03.

44. David Goetz, David Johansen, Margaret Young, Michel Rossignol, Jean-Luc Bourdages, and François Côté, Parliamentary Research Branch, Library of Parliament, *Legislative Summary, Bill C-17: The Public Safety Act, 2002*, November 15, 2002, <www.parl.gc.ca/common/Bills_ls.asp?lang=E&Parl=37&Ses=2&ls=C17&source=Bills_House_Government>, 01/24/03.

45. Department of Justice Canada, Industry Canada, and Solicitor General Canada, *Lawful Access – Consultation Document*, August 25, 2002, <canada.justice.gc.ca/en/cons/la_al/index.html>, 01/24/03.

46. Ibid.

47. Ibid.

48. Llexinformatica Technology Law Society, *Cybercrime and Lawful Access*, <www.lexinformatica.org/cybercrime/>, 02/13/02.

49. Bill Curry, "Minister pushes for border ID cards: No mention of birthplace on 'maple leaf' ID," *National Post,* November 15, 2002, p. A8.

50. "Federal immigration minister suggests ID card might help border problem," *CP Wire*, November 13, 2002. **Note:** As of March 17, 2003, permanent residents (landed immigrants) of Canada who are citizens of a Commonwealth country or Ireland are required to obtain the appropriate visa for travel to the United States.

51. Citizenship and Immigration Canada, *Permanent Resident Card: Issues and Answers*, <www.cic.gc.ca/english/pr%2Dcard/prc%2Dissues.html>, 02/04/03.

52. House of Commons Standing Committee on Citizenship and Immigration, *A National Identity Card: Points on which the Committee Invites Comments*, <www.parl.gc.ca/InfoComDoc/37/2/CIMM/PressReleases/CIMMpr5-e.htm>, 02/04/03.

53. Privacy Commissioner of Canada, *Annual Report to Parliament 2001–2002*, <www.privcom.gc.ca/information/ar/02_04_10_e.asp#>, 03/17/03.

54. Center for Democracy and Technology, *CDT Policy Post*, Volume 7, Number 11, October 26, 2001, <www.cdt.org/publications/pp_7.11.shtml>, 01/29/03.

55. Electronic Frontier Foundation, *Analysis of the Provisions of the USA Patriot Act*.

56. Ibid.

57. Goldstein, "US planning to recruit one in 24 Americans as citizen spies."

58. United States Public Policy Committee, Association for Computing Machinery, *Letter to the Senate Committee on Armed Services*, January 23, 2003, <www.acm.org/usacm/Letters/tia_final.html>. 01/29/03.

59. Jane Black, "Snooping in All the Wrong Places: Not only would the Administration's plan to centralize every American's records destroy privacy, the security payoff would be minimal," *Business Week Online*, December 18, 2002, <www.businessweek.com/technology/content/dec2002/tc20021218_8515.htm>, 01/23/03.

60. Electronic Frontier Foundation, *Analysis of the Provisions of the USA Patriot Act*.

61. George Radwanski, Privacy Commissioner of Canada, *Letter sent to the Honourable Martin Cauchon, Minister of Justice and the Attorney General of Canada, the Honourable Wayne Easter, Solicitor General of Canada, and the Honourable Allan Rock, Minister of Industry, regarding the "Lawful Access" proposals*, November 25, 2002, <www.privcom.gc.ca/media/le_021125_e.asp>, 01/30/03.

62. Electronic Frontier Foundation, *Analysis of the Provisions of the USA Patriot Act*.

63. Canadian Centre for Policy Alternatives, *Analysis Of Bill C-36: An Act To Combat Terrorism*, <www.policyalternatives.ca/publications/c-36.html>, 01/24/03.

64. Privacy Commissioner of Canada, *Annual Report to Parliament 2001–2002*, <www.privcom.gc.ca/information/ar/02_04_10_e.asp#>, 03/17/03.

65. Senators Patrick Leahy, Russell Feingold and Maria Cantwell, *Letter to the Honourable John Ashcroft, Attorney General, United States Department of Justice*, January 10, 2003, <www.fas.org/sgp/news/2003/01/leahy011003.html>, 03/06/03.

66. Jay Stanley and Barry Steinhardt, American Civil Liberties Union, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, January 2003, p. 9, <www.aclu.org/Privacy/Privacy.cfm?ID=11573&c=39#FileAttach>, 01/22/03.

67. Black, "Snooping in All the Wrong Places."

68. OMB Watch, "Restore FOIA Bill: An Important Step in Fixing the Homeland Security Act," March 12, 2003, <www.ombwatch.org/article/articleview/1378/1/18/>, 03/18/03.

69. Charles Levendosky, "Protecting Liberty While Ensuring Homeland Security," *First Amendment Cyber-Tribune*, July 28, 2002, <w3.trib.com/FACT/1st.lev.nixingTIPS.html>, 01/22/03.

70. Jane Black, "Some TIPS for John Ashcroft: Mr. Attorney General, forget your plan for a system to promote Americans spying on Americans. It won't work — and is un-American," *Business Week Online*, July 25, 2002, <www.businessweek.com/bwdaily/dnflash/jul2002/nf20020725_8083.htm>, 01/23/03.

71. Electronic Frontier Foundation, *Analysis of the Provisions of the USA Patriot Act*.

72. Ibid.

73. Ann Cavoukian, Information and Privacy Commissioner/Ontario, *Letter to federal Attorney General Anne McLellan on Bill C-36, the proposed anti-terrorism legislation*, October 30, 2001, <www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11467&N_ID=1&PT_ID=11457&U_ID=0>, 03/06/03.

74. Ibid.

75. Electronic Privacy Information Center, *Letter to Senators Tom Daschle and Trent Lott*, November 18, 2002, <www.epic.org/privacy/profiling/tia/tialetter11.18.02.html>, 01/29/03.

76. Roy Mark, "Senate Kills Funding for Pentagon Data Mining Program," *CIO Information Network*, EarthWeb, January 24, 2003, <cin.earthweb.com/news/article.php/1574251>, 01/29/03.

77. Rowan Scarborough, "Two panels to monitor Pentagon's spy project," *The Washington Times*, February 8, 2003, <www.washtimes.com/national/default-20032825814.htm>, 03/19/03.

78. Shane Harris, "Critics say Defense 'total information awareness' impractical," *Government Executive Magazine*, December 12, 2002, <www.govexec.com/dailyfed/1202/121202h1.htm>, 01/23/03.

79. United States Public Policy Committee, Association for Computing Machinery, *Letter to the Senate Committee on Armed Services*.

80. Bruce Schneier, *Crypto-Gram Newsletter*, October 15, 2001, <www.counterpane.com/crypto-gram-0110.html>, 01/20/03.

81. Jane Black, "Some TIPS for John Ashcroft."

82. Ibid.

83. Charles C. Mann, "Homeland Insecurity," *The Atlantic Monthly*, September 2002, <www.theatlantic.com/issues/2002/09/mann.htm>, 01/20/03.

84. Ibid.

85. Ibid.

86. Ibid.

87. Ibid.

88. United States Public Policy Committee, Association for Computing Machinery, *Letter to the Senate Committee on Armed Services.*

89. Ibid.

90. Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 1997, <www.info-law.com/lost.html>, 05/16/01.

91. Mann, "Homeland Insecurity."

92. Shane Harris, "Counterterrorism project assailed by lawmakers, privacy advocates," *Government Executive Magazine*, November 25, 2002, <www.govexec.com/dailyfed/1102/112502h1.htm>, 01/23/03.

93. Harris, "Critics say Defense 'total information awareness' impractical."

94. Ibid.

95. Black, "Some TIPS for John Ashcroft."

96. Black, "Snooping in All the Wrong Places."

97. Stanley and Steinhardt, *Bigger Monster, Weaker Chains.*

98. Chakrabarti and Strauss, *Carnival Booth.*

99. Ibid.

100. Ibid.

101. Ibid.

102. Ibid.

103. Ibid.

104. Reported in several issues during October 2001. See: <www.msnbc.com/news/NW-attackonamerica_Front.asp?cp1=1>, 03/06/03.

105. Chakrabarti and Strauss, *Carnival Booth*.

106. Ibid.

107. David Carr, "The Futility of 'Homeland Defense'," *The Atlantic Monthly*, January 2002, <www.theatlantic.com/issues/2002/01/carr.htm>, 01/21/03.

108. Mann, "Homeland Insecurity."

109. Ibid.

110. Black, "Snooping in All the Wrong Places."

111. Mann, "Homeland Insecurity."

112. Carr, "The Futility of 'Homeland Defense'."

113. *Constitution Act, 1982* [en. by the Canada Act 1982 (U.K.), 1982, c. 11 Schedule B], as amended.

114. Opinion by Mr. Roger Tassé, O.C., Q.C., November 21, 2002, <www.privcom.gc.ca/media/nr-c/opinion_021122_rt_e.asp>, 01/28/03.

115. Opinion by retired Supreme Court Justice Hon. Gérard V. La Forest, C.C., Q.C., as cited in Privacy Commissioner of Canada, *News Release*, November 22, 2002, <www.privcom.gc.ca/media/nr-c/02_05_b_021122_e.asp>, 01/28/03.

116. David Loukidelis, Information and Privacy Commissioner of British Columbia, *Letter to The Honourable Elinor Caplan, Minister of National Revenue*, October 3, 2002, <www.privcom.gc.ca/media/dl_021003_e.asp>, 01/28/03.

117. Amnesty International (Canada), *Protecting Human Rights and Providing Security: Amnesty International's Comments with Respect to Bill C-36*, <www.amnesty.ca/sept11/C36.htm>, 01/29/03.

118. Nancy Chang, Center for Constitutional Rights, *The USA PATRIOT Act: What's So Patriotic About Trampling on the Bill of Rights?*, November 2001, pp. 2–3, <www.ccr-ny.org/v2/whatsnew/docs/USA_PATRIOT_ACT.pdf>, 01/29/03.

119. Ibid.

120. Michael Ratner, Center for Constitutional Rights, *Making Us Less Free: War on Terrorism or War on Liberty?*, <www.ccr-ny.org/v2/viewpoints/viewpoint.asp?ObjID=YLhsqUx1eu&Content=143>, 01/29/03.

121. Section 11 of the *Charter of Rights and Freedoms*:

> Any person charged with an offence has the right ...
>
> (d) to be presumed innocent until proven guilty according to law in a fair and public hearing by an independent and impartial tribunal.
>
> *Constitution Act*, 1982 [en. by the Canada Act 1982 (U.K.), 1982, c. 11 Schedule B], as amended.

122. United States Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy* (Washington, D.C.: U.S. Government Printing Office, June 1986), p. 88.

123. American Civil Liberties Union, "As Airlines Debut Profiling System, ACLU Launches Web Complaint Form," *Press Release*, December 31, 1997, <archive.aclu.org/news/n123197a.html>, 01/23/03.

124. John Shattuck, "Computer Matching is a Serious Threat to Individual Rights," Communications of the ACM, June 1984, p. 538.

125. Department of Justice, *Backgrounder, Royal Assent of Bill C-36 The Anti-Terrorism Act*, December 18, 2001, <canada.justice.gc.ca/en/news/nr/2001/doc_28217.html>, 02/11/03.

126. Chang, *The USA PATRIOT Act*.

127. In the United States, the Fourth Amendment states the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. FindLaw, *U.S. Constitution: Fourth Amendment*, <caselaw.lp.findlaw.com/data/constitution/amendment04/>, 02/20/03.

128. Chang, *The USA PATRIOT Act*.

129. Ratner, *Making Us Less Free*.

130. Ibid.

131. Ibid.

132. White House Commission on Aviation Safety and Security, *Final Report to President Clinton*, February 17, 1997, <www.airportnet.org/depts/regulatory/gorecom.htm>, as cited in Chakrabarti and Strauss, *Carnival Booth*.

133. Michigan Advisory Committee, *Civil Rights Issues Facing Arab Americans*.

134. American Civil Liberties Union, "As Airlines Debut Profiling System."

135. Black, "Some TIPS for John Ashcroft."

136. David Kilgour, Sam Millar and Jacqueline O'Neill, "Strength Under Siege: Canadian Civil Society Post-September 11th," <www.david-kilgour.com/news/Sept%2011.htm>, 01/27/02.

137. Susan McClelland, "Rising from the fire: Hamilton's religious leaders unite to combat," *Macleans*, <www.macleans.ca/xta-asp/storyview.asp?viewtype=search&tpl=search_frame&edate=2001/10/22&vpath=/xta-doc1/2001/10/22/cover/58590.shtml&maxrec=66&recnum=12&searchtype=BASIC&pg=1&rankbase=90&searchstring=Susan+McClelland>, 01/27/03.

138. Amnesty International (Canada), *Protecting Human Rights and Providing Security*.

139. Ibid.

140. Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992), pp. 12–13.

141. Sheri A. Alpert, "Privacy and Intelligent Highways: Finding the Right of Way," *Santa Clara Computer and High Technology Law Journal — Privacy and ITS*, March 1995, p. 102.

142. *Griswold v. Connecticut*, as cited in Robert Gellman, "Does Privacy Law Work," *Technology and Privacy: The New Landscape*, ed. Philip E. Agree and Marc Rotenberg (Cambridge: The MIT Press, 1998), p. 202.

143. United States Office of Technology Assessment, *Criminal Justice: New Technologies and the Constitution, Special Report* OTA-CIT-366 (Washington D.C.: U.S. Government Printing Office, May 1988), p. 8.

144. *R. v. Dyment* (1988), 55 D.L.R. (4th) 503 at 513 (S.C.C.).

145. House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities, *Privacy: Where do we draw the line? Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities* (Ottawa: Public Works and Government Services Canada, April 1997), p. 6.

146. Law Reform Commission, *Privacy: Background*, Vol. 1, Report No. 22 (Canberra: Australian Government Publishing Service, 1983), p. 21.

147. Department of Communications and Department of Justice, *Privacy & Computers* (Ottawa: Information Canada, 1992), pp. 13 & 14.

148. Gary T. Marx, "Privacy and Technology," <web.mit.edu/gtmarx/www/privantt.html>, 05/23/01.

149. Law Reform Commission, *Privacy*, p. 37.

150. Marx, *Undercover*, p. 223.

151. M.G. Stone and Malcolm Warner, "Politics, Privacy and Computers," The Political Quarterly 40(1969), p. 260, as cited in Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992), p. 29.

152. Gary T. Marx, "Ethics of the New Surveillance," in *Visions of Privacy: Policy Choices for the Digital Age*, ed. Colin J. Bennett and Rebecca Grant (Toronto: University of Toronto Press, 1999), p. 40.

153. Marx, *Undercover*, p. 230.

154. *Websters Third New International Dictionary*, Philip Babcock Gove, Editor in Chief (Springfield, Massachusetts: Merriam-Webster, Inc, 1986) p. 148.

155. Deborah G. Johnson, *Computer Ethics* (Englewood Cliffs, N.J.: Prentice-Hall, 1985), p. 66, as cited in James H. Moor, "How to Invade and Protect Privacy with Computers," *The Information Web: Ethical and Social Implications of Computer Networking*, edited by Carol C. Gould (San Francisco: Westview Press, Inc., 1989), pp. 60–61.

156. Science Council of Canada, *A Workshop on Information Technologies and Personal Privacy in Canada* (Ottawa: Minister of Supply and Services, 1985), p. 9.

157. Jeffery H. Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future," *Santa Clara Computer and High Technology Law Journal — Privacy and ITS*, March 1995, p. 39.

158. Electronic Privacy Information Center, *Free Speech*, <www.epic.org/free_speech/default.html #anonymity>, 03/09/03.

159. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review*, Vol. IV, No. 5, December 15, 1890, <www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html>, 03/08/03.

160. Roger Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues," *Information Technology & People*, Vol. 7, No. 4, December 1994, pp. 6–37, as cited in <www.anu.edu.au/people/Roger.Clarke/DV/HumanID>, 2/11/99.

161. Bennett, *Regulating Privacy*, p. 19.

162. Gary T. Marx, "Police and Democracy," <web.mit.edu/gtmarx/www/dempol.html>, 05/23/01. This version appeared in *Policing, Security and Democracy: Theory and Practice*, Vol. 2, M. Amir and S. Einsten (eds.).

163. Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Ann Arbor: University of Michigan Press, 1971), p. 21, as cited by Bennett, *Regulating Privacy*, p. 29.

164. Law Reform Commission, *Privacy*, pp. 91–92.

165. Office of the Information and Privacy Commissioner/Ontario, *Submission to the Standing Committee on Citizenship and Immigration on the issue of a proposed national identity card*, February 10, 2003, <www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=14049&N_ID=1&PT_ID=11457&U_ID=6752>, 02/20/03.

166. Privacy Commissioner of Canada, *News Release*, November 1, 2002, <www.privcom.gc.ca/media/nr-c/02_05_b_021101_e.asp>, 01/28/03.

167. Privacy Commissioner of Canada, *News Release*, May 1, 2002, <www.privcom.gc.ca/media/nr-c/02_05_b_020501_e.asp>, 01/28/03.

168. Ann Cavoukian, Information and Privacy Commissioner/Ontario, *Letter to The Honourable Elinor Caplan, Minister of National Revenue*, November 12, 2002, <www.ipc.on.ca/userfiles/page_attachments/111202-let.pdf>, 01/30/03.

169. Privacy Commissioner of Canada, *Annual Report to Parliament 2001–2002*, <www.privcom.gc.ca/information/ar/02_04_10_e.asp#>, 03/17/03.

170. Privacy Commissioner of Canada, *News Release regarding the Public Safety Act, Bill C-17*, November 1, 2002, <www.privcom.gc.ca/media/nr-c/02_05_b_021101_e.asp>, 06/03/03.

171. Goldstein, "US planning to recruit one in 24 Americans as citizen spies."

172. U.S. Public Policy Committee, Association for Computing Machinery, *Letter to the Senate Committee on Armed Services*, January 23, 2003, <www.acm.org/usacm/Letters/tia_final.html>, 01/29/03.

173. Nancy Reichman, "Computer Matching: Toward Computerized Systems of Regulations," *Law and Policy*, October 1987, p. 404.

174. Law Reform Commissioner, Privacy, p. 31.

175. Ann Cavoukian, Information and Privacy Commissioner/Ontario, "Public Safety is Paramount," *CBC News Online*, September 21, 2001, <www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=11259&N_ID=1&PT_ID=11257&U_ID=0>, 03/18/03.

176. Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (North Carolina: University of North Carolina Press, 1995), p. 213.

177. Charles D. Raab, "From Balancing to Steering: New Directions for Data Protection," *Visions of Privacy*, p. 83.

178. Ronald Dworkin, *Taking Privacy Seriously* (London, Duckworth, 1977), pp. 197–98, as cited in Raab, "From Balancing to Steering," p. 75.

179. Charles D. Raab, "From Balancing to Steering," p. 73.

180. Marx, "Ethics of the New Surveillance," p. 58.

181. Marx, *Undercover*, pp. 91–92.

182. Alan F. Westin, Privacy and Freedom (New York: Atheneum, 1967), pp. 370.

183. Regan, Legislating Privacy, p. 217.

184. Ibid., p. 225.

185. Fernando Volio, "Legal personality, privacy and the family," in *The International Bill of Rights* (New York: Columbia University Press, 1981), Henkin (ed), as cited in Global Internet Library Campaign, "Privacy and Human Rights," <www.gilc.org/privacy/survey/intro.html>, 05/16/01.

186. Global Internet Library Campaign, "Privacy and Human Rights," <www.gilc.org/privacy/survey/intro.html>, 05/16/01.

187. Regan, *Legislating Privacy*. p. 225.

188. Ibid., pp. 225–226.

189. Ibid., p. 226.

190. Ibid.

191. Oscar H. Gandy, Jr., *The Pantoptic Sort: A Political Economy of Personal Information* (Boulder: Westview Press, 1993), p. 3, as cited in Regan, *Legislating Privacy*, p. 227.

192. H. Packer, *The Limits of the Criminal Sanction* (Stanford: Stanford University Press, 1968) as cited in Marx, *Undercover*, p. 249.

193. Office of the Information and Privacy Commissioner/Ontario, *Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift*, June 2002, <www.ipc.on.ca/docs/steps.pdf>, 03/11/03.

194. United States Department of Energy, "3-D holographic scanner for better airport security," *RESEARCH News*, September 24, 2001, <www.eurekalert.org/features/doe/2001-09/dnnl-3hs061902.php>, 03/12/03.

195. Office of the Information and Privacy Commissioner/Ontario, *Security Technologies Enabling Privacy (STEPs): Time for a Paradigm Shift.*

196. Westin, *Privacy and Freedom*, p. 398.

197. Henry David Thoreau, *Walden*, 1854, <sdg.lcs.mit.edu/~dnj/walden.html>, 07/02/01.

198. *R. v. Araujo*, [2000]2 S.C.R. 992, Online: LexUM, University of Montreal, Facility of Law, <www.lexum.umontreal.ca/index_en.html>, 06/09/01.

199. Marx, Undercover, p. 105 and Marx, "Privacy and Technology," <web.mit.edu/gtmarx/www/privantt.html>, 05/23/01.

200. Kenneth C. Laudon, *Dossier Society: Value Choices in the Design of National Information Systems* (New York: Columbia University Press, 1986), p. 259.

201. Donald A. Marchand, *The Politics of Privacy, Computers, and Criminal Justice Records: Controlling the Social Costs of Technological Change* (Arlington: Information Resource Press, 1980), p. 5.

202. Marx, "Police and Democracy," <web.mit.edu/gtmarx/www/dempol.html>, 05/23/01.

203. Cavoukian, "Public Safety is Paramount."

204. George Radwanski, Privacy Commissioner of Canada, *Letter to the Honourable Martin Cauchon, Minister of Justice and the Attorney General of Canada, the Honourable Wayne Easter, Solicitor General of Canada, and the Honourable Allan Rock, Minister of Industry, regarding the "Lawful Access" proposals*, November 25, 2002, <www.privcom.gc.ca/media/le_021125_e.asp>, 01/30/03.

205. Office of the Information and Privacy Commissioner/Ontario and the United States Department of Justice, Office of Justice Programs, *Privacy Design Principles for an Integrated Justice System*, <www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&U_id=0&P_ID=11389>, 06/01/01.

206. Commission on Freedom of Information and Individual Privacy, *Public Government for Private People: Protection of Privacy*, Vol. 3 (Toronto: Queen's Printer of Ontario, 1980), pp. 557 & 558.

207. Office of the Information and Privacy Commissioner/Ontario and the United States Department of Justice, Office of Justice Programs, *Privacy Design Principles for an Integrated Justice System.*

208. James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, <www.cdt.org/publications/lawreview/1997albany.shtml>, 05/16/01.

209. Ibid.

210. Laudon, *Dossier Society*, pp. 177, 261 and 265.

211. Ibid., p. 388.

212. Ibid., p. 177.

213. Thilo Weichert, "Public Video Surveillance in View of the European Privacy Protection Directive and German Privacy Protection Law," Remarks at Video Surveillance – A Crime Prevention Instrument in European Comparison Conference, February 22–24, 2000, University of Göttingen, <www.datenschutzzentrum.de/material/themen/video/vidsur_e.htm>, 03/12/03.

214. Marx, "Privacy and Technology," <web.mit.edu/gtmarx/www/privantt.html>, 05/23/01.

215. Laudon, *Dossier Society*, p. 264.

216. Lásló Majtényi, Parliamentary Commissioner for Data Protection and Freedom of Information, Hungary, "Data Protection in the Era of Change of the Political System," 19th International Conference Privacy Data Protection Commissioners, 1997, <www.privacy.fgov.be/conference/pt8_2.html>, 05/16/01.

217. Westin. *Privacy and Freedom*. p. 22.

218. American Civil Liberties Union, *Letter to President Clinton: Veto Terrorism Bill, Preserve Our Greatest Liberty*, April 17, 1996, <www.eff.org/Privacy/Surveillance/Terrorism_militias/960417_aclu_clinton.letter>, 03/11/03.

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: www.ipc.on.ca